



## Clustered Data ONTAP<sup>®</sup> 8.2

### Commands: Manual Page Reference

---

## Contents

Copyright .....	24
Trademarks .....	25
About the Clustered Data ONTAP® 8.2 Commands: Manual Page Reference .....	26
cd .....	27
exit .....	28
history .....	28
man .....	30
redo .....	30
rows .....	32
set .....	33
top .....	36
up .....	37
cluster create .....	38
cluster join .....	39
cluster modify .....	40
cluster ping-cluster .....	42
cluster setup .....	44
cluster show .....	48
cluster unjoin .....	49
cluster contact-info modify .....	49
cluster contact-info show .....	52
cluster date modify .....	53
cluster date show .....	54
cluster ha modify .....	57
cluster ha show .....	57
cluster identity modify .....	58
cluster identity show .....	59
cluster peer create .....	60
cluster peer delete .....	63
cluster peer modify .....	64
cluster peer ping .....	65
cluster peer show .....	68
cluster peer health show .....	70
cluster peer job delete .....	73
cluster peer job pause .....	74
cluster peer job resume .....	75
cluster peer job show .....	76

---

cluster peer job stop .....	80
cluster peer job watch-progress .....	81
cluster ring show .....	81
cluster statistics show .....	84
dashboard alarm show .....	87
dashboard alarm thresholds modify .....	89
dashboard alarm thresholds show .....	90
dashboard health vserver show-aggregate .....	92
dashboard health vserver show-combined .....	94
dashboard health vserver show-lif .....	96
dashboard health vserver show-port .....	97
dashboard health vserver show-protocol .....	99
dashboard health vserver show-volume .....	101
dashboard health vserver show .....	103
dashboard performance show .....	107
dashboard storage show .....	110
event config modify .....	115
event config show .....	117
event destination create .....	118
event destination delete .....	121
event destination modify .....	123
event destination show .....	126
event log show .....	129
event mailhistory delete .....	134
event mailhistory show .....	135
event route add-destinations .....	137
event route modify .....	139
event route remove-destinations .....	141
event route show .....	142
event snmphistory delete .....	145
event snmphistory show .....	146
event status show .....	148
job delete .....	152
job pause .....	153
job resume .....	154
job show-bynode .....	155
job show-cluster .....	157
job show-completed .....	161
job show .....	164
job stop .....	168
job unclaim .....	169
job watch-progress .....	170
job history show .....	170

---

---

job initstate show .....	174
job private delete .....	177
job private pause .....	178
job private resume .....	179
job private show-completed .....	180
job private show .....	183
job private stop .....	186
job private watch-progress .....	186
job schedule delete .....	187
job schedule show-jobs .....	189
job schedule show .....	191
job schedule cron create .....	192
job schedule cron delete .....	193
job schedule cron modify .....	194
job schedule cron show .....	196
job schedule interval create .....	198
job schedule interval delete .....	200
job schedule interval modify .....	201
job schedule interval show .....	203
lun create .....	205
lun delete .....	209
lun map .....	211
lun maxsize .....	213
lun modify .....	216
lun move .....	219
lun resize .....	221
lun show .....	224
lun unmap .....	229
lun bind create .....	230
lun bind destroy .....	231
lun bind show .....	232
lun igroup add .....	234
lun igroup bind .....	236
lun igroup create .....	238
lun igroup delete .....	241
lun igroup disable-aix-support .....	242
lun igroup modify .....	243
lun igroup remove .....	245
lun igroup rename .....	247
lun igroup show .....	248
lun igroup unbind .....	250
lun mapped show .....	251
lun persistent-reservation clear .....	254

---

---

lun persistent-reservation show .....	255
lun portset add .....	258
lun portset create .....	259
lun portset delete .....	261
lun portset remove .....	263
lun portset show .....	264
network ping .....	266
network traceroute .....	267
network connections active show-clients .....	270
network connections active show-lifs .....	272
network connections active show-protocols .....	274
network connections active show-services .....	276
network connections active show .....	278
network connections listening show .....	281
network fcp adapter modify .....	284
network fcp adapter show .....	286
network interface create .....	289
network interface delete .....	294
network interface migrate-all .....	295
network interface migrate .....	296
network interface modify .....	297
network interface rename .....	302
network interface revert .....	302
network interface show-routing-group .....	304
network interface show-zones .....	306
network interface show .....	308
network interface start-cluster-check .....	313
network interface failover-groups create .....	314
network interface failover-groups delete .....	315
network interface failover-groups rename .....	315
network interface failover-groups show .....	316
network options ipv6 modify .....	318
network options ipv6 show .....	318
network options switchless-cluster modify .....	319
network options switchless-cluster show .....	319
network port delete .....	321
network port modify .....	321
network port show .....	323
network port ifgrp add-port .....	327
network port ifgrp create .....	329
network port ifgrp delete .....	331
network port ifgrp remove-port .....	332
network port ifgrp show .....	332

---

---

network port vlan create .....	335
network port vlan delete .....	335
network port vlan show .....	336
network routing-groups create .....	338
network routing-groups delete .....	340
network routing-groups show .....	341
network routing-groups route create .....	343
network routing-groups route delete .....	344
network routing-groups route show .....	344
qos policy-group create .....	347
qos policy-group delete .....	349
qos policy-group modify .....	350
qos policy-group rename .....	351
qos policy-group show .....	352
qos statistics characteristics show .....	354
qos statistics latency show .....	356
qos statistics performance show .....	358
qos statistics resource cpu show .....	360
qos statistics resource disk show .....	362
qos statistics workload characteristics show .....	364
qos statistics workload latency show .....	366
qos statistics workload performance show .....	368
qos statistics workload resource cpu show .....	370
qos statistics workload resource disk show .....	372
security snmpusers .....	374
security audit modify .....	376
security audit show .....	377
security certificate create .....	378
security certificate delete .....	380
security certificate generate-csr .....	382
security certificate install .....	384
security certificate show .....	386
security certificate sign .....	390
security certificate ca-issued revoke .....	393
security certificate ca-issued show .....	394
security login create .....	397
security login delete .....	399
security login lock .....	400
security login modify .....	401
security login password .....	402
security login show .....	403
security login unlock .....	405
security login domain-tunnel create .....	405

---

---

security login domain-tunnel delete .....	407
security login domain-tunnel modify .....	408
security login domain-tunnel show .....	409
security login publickey create .....	410
security login publickey delete .....	412
security login publickey load-from-uri .....	412
security login publickey modify .....	415
security login publickey show .....	417
security login role create .....	419
security login role delete .....	421
security login role modify .....	421
security login role show-ontapi .....	422
security login role show .....	424
security login role config modify .....	426
security login role config reset .....	428
security login role config show .....	428
security ssl modify .....	432
security ssl show .....	434
snapmirror abort .....	436
snapmirror break .....	439
snapmirror create .....	442
snapmirror delete .....	447
snapmirror initialize-ls-set .....	450
snapmirror initialize .....	452
snapmirror list-destinations .....	457
snapmirror modify .....	461
snapmirror promote .....	465
snapmirror quiesce .....	468
snapmirror release .....	471
snapmirror restore .....	473
snapmirror resume .....	478
snapmirror resync .....	481
snapmirror show .....	487
snapmirror update-ls-set .....	498
snapmirror update .....	501
snapmirror policy add-rule .....	506
snapmirror policy create .....	507
snapmirror policy delete .....	510
snapmirror policy modify-rule .....	510
snapmirror policy modify .....	512
snapmirror policy remove-rule .....	514
snapmirror policy show .....	515
snapmirror snapshot-owner create .....	518

---

---

snapmirror snapshot-owner delete .....	520
snapmirror snapshot-owner show .....	522
statistics show-periodic .....	524
statistics show .....	527
statistics start .....	530
statistics stop .....	532
statistics catalog counter show .....	533
statistics catalog instance show .....	535
statistics catalog object show .....	537
statistics oncrpc show-replay-cache .....	539
statistics oncrpc show-rpc-calls .....	541
statistics samples delete .....	544
statistics samples show .....	545
statistics secd show .....	547
statistics settings modify .....	550
statistics settings show .....	551
statistics striping show-summary .....	552
statistics striping show .....	555
storage aggregate add-disks .....	558
storage aggregate create .....	562
storage aggregate delete .....	565
storage aggregate modify .....	566
storage aggregate offline .....	569
storage aggregate online .....	570
storage aggregate rename .....	571
storage aggregate restrict .....	571
storage aggregate scrub .....	573
storage aggregate show-scrub-status .....	575
storage aggregate show-space .....	577
storage aggregate show .....	580
storage aggregate 64bit-upgrade status .....	586
storage aggregate relocation show .....	589
storage aggregate relocation start .....	591
storage array modify .....	592
storage array remove .....	593
storage array rename .....	594
storage array show .....	594
storage array config show .....	597
storage array port modify .....	600
storage array port remove .....	600
storage array port show .....	601
storage disk assign .....	605
storage disk fail .....	608

---



---

storage disk modify .....	610
storage disk reassign .....	612
storage disk remove .....	614
storage disk removeowner .....	615
storage disk replace .....	615
storage disk set-led .....	618
storage disk show .....	620
storage disk unfail .....	635
storage disk updatefirmware .....	635
storage disk zerospares .....	637
storage disk option modify .....	637
storage disk option show .....	640
storage errors show .....	642
storage failover giveback .....	644
storage failover modify .....	647
storage failover show-giveback .....	652
storage failover show-takeover .....	654
storage failover show .....	658
storage failover takeover .....	678
storage failover hwassist show .....	680
storage failover hwassist test .....	683
storage failover hwassist stats clear .....	684
storage failover hwassist stats show .....	684
storage failover interconnect show-link .....	686
storage failover interconnect status .....	688
storage failover interconnect statistics error show .....	690
storage failover interconnect statistics performance basic .....	692
storage failover interconnect statistics performance vi-if .....	694
storage failover internal-options modify .....	696
storage failover internal-options show .....	696
storage failover mailbox-disk show .....	701
storage failover progress-table show .....	703
storage firmware download .....	705
storage library config show .....	707
storage library path show-by-initiator .....	709
storage library path show .....	711
storage load balance .....	714
storage load show .....	715
storage path quiesce .....	718
storage path resume .....	719
storage path show-by-initiator .....	719
storage path show .....	722
storage raid-options modify .....	727

---

---

storage raid-options show .....	728
system configuration backup copy .....	730
system configuration backup create .....	731
system configuration backup delete .....	732
system configuration backup download .....	733
system configuration backup rename .....	734
system configuration backup show .....	735
system configuration backup upload .....	737
system configuration backup settings modify .....	737
system configuration backup settings set-password .....	739
system configuration backup settings show .....	740
system configuration recovery cluster recreate .....	742
system configuration recovery cluster rejoin .....	743
system configuration recovery cluster sync .....	744
system configuration recovery node restore .....	745
system health alert delete .....	747
system health alert modify .....	747
system health alert show .....	749
system health alert definition show .....	752
system health autosupport trigger history show .....	755
system health cluster-switch create .....	758
system health cluster-switch delete .....	760
system health cluster-switch modify .....	760
system health cluster-switch show .....	761
system health cluster-switch fan show .....	763
system health cluster-switch interface show .....	766
system health cluster-switch polling-interval modify .....	769
system health cluster-switch polling-interval show .....	769
system health cluster-switch power show .....	770
system health cluster-switch temperature show .....	772
system health cluster-switch utilization show .....	774
system health config show .....	776
system health node-connectivity adapter show .....	778
system health node-connectivity disk show .....	782
system health node-connectivity shelf show .....	785
system health policy definition modify .....	788
system health policy definition show .....	788
system health status show .....	792
system health subsystem show .....	792
system health system-connectivity shelf show .....	795
system license add .....	797
system license clean-up .....	797
system license delete .....	799

---

---

system license show .....	799
system license status show .....	802
system node halt .....	804
system node modify .....	806
system node reboot .....	808
system node rename .....	809
system node revert-to .....	811
system node run .....	811
system node show .....	814
system node systemshell .....	817
system node autosupport invoke .....	819
system node autosupport modify .....	821
system node autosupport show .....	826
system node autosupport destinations show .....	831
system node autosupport history retransmit .....	833
system node autosupport history show .....	835
system node autosupport manifest show .....	838
system node autosupport trigger modify .....	843
system node autosupport trigger show .....	845
system node coredump delete-all .....	848
system node coredump delete .....	848
system node coredump save-all .....	849
system node coredump save .....	851
system node coredump show .....	852
system node coredump status .....	855
system node coredump upload .....	860
system node coredump config modify .....	862
system node coredump config show .....	863
system node coredump reports delete .....	865
system node coredump reports show .....	865
system node coredump reports upload .....	868
system node coredump segment delete-all .....	869
system node coredump segment delete .....	869
system node coredump segment show .....	870
system node coredump segment start .....	873
system node coredump segment status .....	873
system node coredump segment stop .....	876
system node coredump segment config modify .....	876
system node coredump segment config show .....	877
system node environment sensors show .....	879
system node firmware download .....	883
system node hardware tape drive show .....	883
system node hardware tape library show .....	886

---

---

system node image get .....	888
system node image modify .....	889
system node image show-update-progress .....	889
system node image show .....	891
system node image update .....	893
system node image package delete .....	896
system node image package show .....	896
system node platform ifswitch stat .....	898
system node platform ifswitch mode modify .....	900
system node platform ifswitch mode show .....	901
system node root-mount create .....	901
system node root-mount delete .....	903
system node root-mount show .....	904
system node service-processor reboot-sp .....	906
system node service-processor show .....	907
system node service-processor image modify .....	910
system node service-processor image show .....	911
system node service-processor image update .....	914
system node service-processor image update-progress show .....	916
system node service-processor network modify .....	918
system node service-processor network show .....	921
system node upgrade-revert show .....	925
system node upgrade-revert upgrade .....	928
system script delete .....	928
system script show .....	930
system script start .....	932
system script stop .....	933
system script upload .....	934
system services firewall modify .....	935
system services firewall show .....	935
system services firewall policy clone .....	937
system services firewall policy create .....	937
system services firewall policy delete .....	940
system services firewall policy modify .....	941
system services firewall policy show .....	942
system services manager install show .....	944
system services manager policy add .....	946
system services manager policy remove .....	946
system services manager policy setstate .....	947
system services manager policy show .....	949
system services manager status show .....	951
system services ndmp kill-all .....	953
system services ndmp kill .....	953

---

---

system services ndmp modify .....	955
system services ndmp off .....	956
system services ndmp on .....	958
system services ndmp password .....	959
system services ndmp probe .....	959
system services ndmp show .....	963
system services ndmp start .....	965
system services ndmp status .....	966
system services ndmp stop .....	971
system services ndmp terminate .....	973
system services ndmp log start .....	974
system services ndmp log stop .....	976
system services ndmp node-scope-mode off .....	977
system services ndmp node-scope-mode on .....	978
system services ndmp node-scope-mode status .....	978
system services ntp server create .....	979
system services ntp server delete .....	980
system services ntp server modify .....	980
system services ntp server show .....	981
system services web modify .....	984
system services web show .....	986
system services web node show .....	988
system smtape abort .....	991
system smtape backup .....	992
system smtape break .....	994
system smtape continue .....	995
system smtape restore .....	996
system smtape showheader .....	998
system smtape status clear .....	1001
system smtape status show .....	1002
system snmp authtrap .....	1006
system snmp contact .....	1007
system snmp init .....	1008
system snmp location .....	1008
system snmp show .....	1010
system snmp community add .....	1011
system snmp community delete .....	1012
system snmp community show .....	1013
system snmp traphost add .....	1013
system snmp traphost delete .....	1015
system snmp traphost show .....	1016
system timeout modify .....	1016
system timeout show .....	1017

---

---

volume autosize .....	1018
volume create .....	1021
volume delete .....	1030
volume make-vsroot .....	1032
volume modify .....	1032
volume mount .....	1045
volume offline .....	1046
volume online .....	1047
volume rename .....	1048
volume restrict .....	1048
volume show-footprint .....	1050
volume show-space .....	1055
volume show .....	1061
volume size .....	1078
volume unmount .....	1079
volume clone create .....	1080
volume clone show .....	1083
volume clone split estimate .....	1089
volume clone split show .....	1093
volume clone split start .....	1095
volume clone split stop .....	1096
volume copy start .....	1096
volume efficiency check .....	1097
volume efficiency modify .....	1098
volume efficiency off .....	1100
volume efficiency on .....	1101
volume efficiency revert-to .....	1102
volume efficiency show .....	1103
volume efficiency start .....	1110
volume efficiency stat .....	1112
volume efficiency stop .....	1116
volume efficiency undo .....	1116
volume efficiency policy create .....	1119
volume efficiency policy delete .....	1121
volume efficiency policy modify .....	1121
volume efficiency policy show .....	1123
volume file modify .....	1126
volume file reservation .....	1127
volume file show-disk-usage .....	1127
volume file show-filehandle .....	1131
volume file clone autodelete .....	1133
volume file clone clear .....	1134
volume file clone create .....	1135

---

---

volume file clone status .....	1137
volume file clone stop .....	1138
volume flexcache create .....	1139
volume flexcache delete .....	1141
volume flexcache show .....	1142
volume flexcache cache-policy create .....	1145
volume flexcache cache-policy delete .....	1147
volume flexcache cache-policy modify .....	1147
volume flexcache cache-policy show .....	1150
volume move abort .....	1152
volume move show .....	1154
volume move start .....	1160
volume move trigger-cutover .....	1161
volume move target-aggr show .....	1163
volume qtree create .....	1165
volume qtree delete .....	1166
volume qtree modify .....	1168
volume qtree oplocks .....	1169
volume qtree rename .....	1171
volume qtree security .....	1172
volume qtree show .....	1174
volume qtree statistics-reset .....	1177
volume qtree statistics .....	1177
volume quota modify .....	1181
volume quota off .....	1184
volume quota on .....	1185
volume quota report .....	1187
volume quota resize .....	1193
volume quota show .....	1195
volume quota policy copy .....	1200
volume quota policy create .....	1200
volume quota policy delete .....	1201
volume quota policy rename .....	1202
volume quota policy show .....	1203
volume quota policy rule create .....	1205
volume quota policy rule delete .....	1210
volume quota policy rule modify .....	1212
volume quota policy rule show .....	1215
volume snapshot compute-reclaimable .....	1218
volume snapshot create .....	1219
volume snapshot delete .....	1220
volume snapshot modify .....	1221
volume snapshot partial-restore-file .....	1222

---

---

volume snapshot rename .....	1224
volume snapshot restore-file .....	1226
volume snapshot restore .....	1227
volume snapshot show .....	1229
volume snapshot autodelete modify .....	1235
volume snapshot autodelete show .....	1239
volume snapshot policy add-schedule .....	1242
volume snapshot policy create .....	1244
volume snapshot policy delete .....	1248
volume snapshot policy modify-schedule .....	1248
volume snapshot policy modify .....	1249
volume snapshot policy remove-schedule .....	1250
volume snapshot policy show .....	1251
vserver context .....	1254
vserver create .....	1255
vserver delete .....	1258
vserver modify .....	1258
vserver rename .....	1261
vserver setup .....	1261
vserver show .....	1266
vserver start .....	1271
vserver stop .....	1271
vserver audit create .....	1272
vserver audit delete .....	1275
vserver audit disable .....	1275
vserver audit enable .....	1276
vserver audit modify .....	1276
vserver audit show .....	1279
vserver cifs create .....	1282
vserver cifs delete .....	1284
vserver cifs modify .....	1284
vserver cifs nbtstat .....	1286
vserver cifs password-change .....	1290
vserver cifs password-reset .....	1290
vserver cifs show .....	1291
vserver cifs start .....	1294
vserver cifs stop .....	1295
vserver cifs branchcache create .....	1295
vserver cifs branchcache delete .....	1298
vserver cifs branchcache hash-create .....	1298
vserver cifs branchcache hash-flush .....	1299
vserver cifs branchcache modify .....	1300
vserver cifs branchcache show .....	1303

---



---

vserver cifs domain discovered-servers reset-servers .....	1305
vserver cifs domain discovered-servers show .....	1305
vserver cifs domain preferred-dc add .....	1308
vserver cifs domain preferred-dc remove .....	1309
vserver cifs domain preferred-dc show .....	1309
vserver cifs group-policy modify .....	1311
vserver cifs group-policy show-applied .....	1311
vserver cifs group-policy show-defined .....	1314
vserver cifs group-policy show .....	1317
vserver cifs group-policy update .....	1318
vserver cifs home-directory search-path add .....	1318
vserver cifs home-directory search-path remove .....	1319
vserver cifs home-directory search-path reorder .....	1319
vserver cifs home-directory search-path show .....	1320
vserver cifs options modify .....	1321
vserver cifs options show .....	1325
vserver cifs security modify .....	1328
vserver cifs security show .....	1330
vserver cifs session show .....	1332
vserver cifs session file show .....	1336
vserver cifs share create .....	1340
vserver cifs share delete .....	1344
vserver cifs share modify .....	1344
vserver cifs share show .....	1347
vserver cifs share access-control create .....	1351
vserver cifs share access-control delete .....	1352
vserver cifs share access-control modify .....	1352
vserver cifs share access-control show .....	1353
vserver cifs share properties add .....	1356
vserver cifs share properties remove .....	1358
vserver cifs share properties show .....	1359
vserver cifs superuser create .....	1362
vserver cifs superuser delete .....	1362
vserver cifs superuser show .....	1363
vserver cifs symlink create .....	1365
vserver cifs symlink delete .....	1367
vserver cifs symlink modify .....	1367
vserver cifs symlink show .....	1370
vserver cifs users-and-groups update-names .....	1372
vserver cifs users-and-groups local-group add-members .....	1374
vserver cifs users-and-groups local-group create .....	1375
vserver cifs users-and-groups local-group delete .....	1376
vserver cifs users-and-groups local-group modify .....	1376

---

---

vserver cifs users-and-groups local-group remove-members .....	1377
vserver cifs users-and-groups local-group rename .....	1379
vserver cifs users-and-groups local-group show-members .....	1380
vserver cifs users-and-groups local-group show .....	1382
vserver cifs users-and-groups local-user create .....	1384
vserver cifs users-and-groups local-user delete .....	1385
vserver cifs users-and-groups local-user modify .....	1387
vserver cifs users-and-groups local-user rename .....	1387
vserver cifs users-and-groups local-user set-password .....	1389
vserver cifs users-and-groups local-user show-membership .....	1391
vserver cifs users-and-groups local-user show .....	1393
vserver cifs users-and-groups privilege add-privilege .....	1395
vserver cifs users-and-groups privilege remove-privilege .....	1396
vserver cifs users-and-groups privilege reset-privilege .....	1398
vserver cifs users-and-groups privilege show .....	1400
vserver data-policy export .....	1402
vserver data-policy import .....	1403
vserver data-policy validate .....	1404
vserver export-policy copy .....	1405
vserver export-policy create .....	1405
vserver export-policy delete .....	1407
vserver export-policy rename .....	1407
vserver export-policy show .....	1408
vserver export-policy rule create .....	1410
vserver export-policy rule delete .....	1417
vserver export-policy rule modify .....	1418
vserver export-policy rule setindex .....	1424
vserver export-policy rule show .....	1426
vserver fcp create .....	1433
vserver fcp delete .....	1435
vserver fcp modify .....	1436
vserver fcp show .....	1438
vserver fcp start .....	1439
vserver fcp stop .....	1440
vserver fcp initiator show .....	1441
vserver fcp interface show .....	1443
vserver fcp portname set .....	1446
vserver fcp portname show .....	1448
vserver fcp wwpn-alias remove .....	1450
vserver fcp wwpn-alias set .....	1451
vserver fcp wwpn-alias show .....	1453
vserver fpolicy disable .....	1455
vserver fpolicy enable .....	1456

---

---

vserver fpolicy engine-connect .....	1458
vserver fpolicy engine-disconnect .....	1460
vserver fpolicy show-enabled .....	1462
vserver fpolicy show-engine .....	1464
vserver fpolicy show .....	1467
vserver fpolicy policy create .....	1469
vserver fpolicy policy delete .....	1471
vserver fpolicy policy modify .....	1471
vserver fpolicy policy show .....	1474
vserver fpolicy policy event create .....	1477
vserver fpolicy policy event delete .....	1482
vserver fpolicy policy event modify .....	1482
vserver fpolicy policy event show .....	1488
vserver fpolicy policy external-engine create .....	1490
vserver fpolicy policy external-engine delete .....	1495
vserver fpolicy policy external-engine modify .....	1496
vserver fpolicy policy external-engine show .....	1501
vserver fpolicy policy scope create .....	1505
vserver fpolicy policy scope delete .....	1509
vserver fpolicy policy scope modify .....	1509
vserver fpolicy policy scope show .....	1514
vserver group-mapping create .....	1517
vserver group-mapping delete .....	1519
vserver group-mapping insert .....	1519
vserver group-mapping modify .....	1521
vserver group-mapping show .....	1522
vserver group-mapping swap .....	1525
vserver iscsi create .....	1526
vserver iscsi delete .....	1528
vserver iscsi modify .....	1529
vserver iscsi show .....	1532
vserver iscsi start .....	1535
vserver iscsi stop .....	1536
vserver iscsi command show .....	1537
vserver iscsi connection show .....	1539
vserver iscsi connection shutdown .....	1542
vserver iscsi initiator show .....	1543
vserver iscsi interface disable .....	1545
vserver iscsi interface enable .....	1546
vserver iscsi interface show .....	1547
vserver iscsi interface accesslist add .....	1550
vserver iscsi interface accesslist remove .....	1552
vserver iscsi interface accesslist show .....	1554

---

---

vserver iscsi isns create .....	1556
vserver iscsi isns delete .....	1558
vserver iscsi isns disable .....	1559
vserver iscsi isns modify .....	1560
vserver iscsi isns show .....	1562
vserver iscsi isns start .....	1564
vserver iscsi isns stop .....	1565
vserver iscsi isns update .....	1566
vserver iscsi security create .....	1567
vserver iscsi security default .....	1569
vserver iscsi security delete .....	1571
vserver iscsi security generate .....	1572
vserver iscsi security modify .....	1573
vserver iscsi security show .....	1575
vserver iscsi session show .....	1577
vserver iscsi session shutdown .....	1581
vserver iscsi session parameter show .....	1582
vserver locks break .....	1586
vserver locks show .....	1587
vserver name-mapping create .....	1595
vserver name-mapping delete .....	1597
vserver name-mapping insert .....	1597
vserver name-mapping modify .....	1599
vserver name-mapping show .....	1600
vserver name-mapping swap .....	1602
vserver nfs create .....	1602
vserver nfs delete .....	1610
vserver nfs modify .....	1610
vserver nfs off .....	1618
vserver nfs on .....	1618
vserver nfs show .....	1619
vserver nfs start .....	1627
vserver nfs status .....	1627
vserver nfs stop .....	1628
vserver nfs kerberos-config modify .....	1628
vserver nfs kerberos-config show .....	1631
vserver peer accept .....	1633
vserver peer create .....	1634
vserver peer delete .....	1636
vserver peer modify .....	1637
vserver peer reject .....	1638
vserver peer resume .....	1639
vserver peer show-all .....	1640

---

---

vserver peer show .....	1642
vserver peer suspend .....	1644
vserver peer transition create .....	1645
vserver peer transition delete .....	1646
vserver peer transition modify .....	1647
vserver peer transition show .....	1648
vserver security file-directory apply .....	1650
vserver security file-directory show .....	1651
vserver security file-directory job show .....	1656
vserver security file-directory ntfs create .....	1660
vserver security file-directory ntfs delete .....	1663
vserver security file-directory ntfs modify .....	1663
vserver security file-directory ntfs show .....	1666
vserver security file-directory ntfs dacl add .....	1668
vserver security file-directory ntfs dacl modify .....	1672
vserver security file-directory ntfs dacl remove .....	1676
vserver security file-directory ntfs dacl show .....	1677
vserver security file-directory ntfs sacl add .....	1681
vserver security file-directory ntfs sacl modify .....	1685
vserver security file-directory ntfs sacl remove .....	1689
vserver security file-directory ntfs sacl show .....	1690
vserver security file-directory policy create .....	1694
vserver security file-directory policy delete .....	1696
vserver security file-directory policy show .....	1696
vserver security file-directory policy task add .....	1698
vserver security file-directory policy task modify .....	1701
vserver security file-directory policy task remove .....	1704
vserver security file-directory policy task show .....	1704
vserver security trace filter create .....	1707
vserver security trace filter delete .....	1708
vserver security trace filter modify .....	1710
vserver security trace filter show .....	1711
vserver security trace trace-result delete .....	1714
vserver security trace trace-result show .....	1714
vserver services dns create .....	1721
vserver services dns delete .....	1722
vserver services dns modify .....	1723
vserver services dns show .....	1725
vserver services dns hosts create .....	1727
vserver services dns hosts delete .....	1727
vserver services dns hosts modify .....	1728
vserver services dns hosts show .....	1729
vserver services kerberos-realm create .....	1731

---

---

vserver services kerberos-realm delete .....	1733
vserver services kerberos-realm modify .....	1733
vserver services kerberos-realm show .....	1736
vserver services ldap create .....	1739
vserver services ldap delete .....	1740
vserver services ldap modify .....	1740
vserver services ldap show .....	1742
vserver services ldap client create .....	1743
vserver services ldap client delete .....	1746
vserver services ldap client modify-bind-password .....	1746
vserver services ldap client modify .....	1747
vserver services ldap client show .....	1751
vserver services ldap client schema copy .....	1754
vserver services ldap client schema delete .....	1754
vserver services ldap client schema modify .....	1755
vserver services ldap client schema show .....	1758
vserver services ndmp generate-password .....	1761
vserver services ndmp kill-all .....	1762
vserver services ndmp kill .....	1762
vserver services ndmp modify .....	1764
vserver services ndmp off .....	1770
vserver services ndmp on .....	1777
vserver services ndmp probe .....	1784
vserver services ndmp show .....	1787
vserver services ndmp status .....	1796
vserver services ndmp log start .....	1802
vserver services ndmp log stop .....	1804
vserver services netgroup load .....	1804
vserver services netgroup status .....	1805
vserver services nis-domain create .....	1807
vserver services nis-domain delete .....	1808
vserver services nis-domain modify .....	1809
vserver services nis-domain show .....	1811
vserver services unix-group adduser .....	1813
vserver services unix-group create .....	1813
vserver services unix-group delete .....	1814
vserver services unix-group deluser .....	1815
vserver services unix-group load-from-uri .....	1815
vserver services unix-group modify .....	1816
vserver services unix-group show .....	1817
vserver services unix-user create .....	1819
vserver services unix-user delete .....	1819
vserver services unix-user load-from-uri .....	1820

---

---

vserver services unix-user modify .....	1821
vserver services unix-user show .....	1822
vserver services web modify .....	1824
vserver services web show .....	1826
vserver services web access create .....	1829
vserver services web access delete .....	1830
vserver services web access show .....	1831
vserver smtape break .....	1833

---

## Copyright

Copyright © 1994-2013 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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



---

## Trademarks

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.

---

## About the Clustered Data ONTAP® 8.2 Commands: Manual Page Reference

The Clustered Data ONTAP® 8.2 Commands: Manual Page Reference document is a compilation of all the manual (man) pages for clustered Data ONTAP commands.

It includes admin and advanced level commands.

Manual pages are grouped into sections according to families to which the commands belong.

### Viewing manual pages at the command line

To view a manual page for a command at your storage system command line (console), enter the following:

```
man command
```

Note: Data ONTAP commands are case-sensitive.

To see a list of all commands from the storage system command line, enter a question mark (?) after the host prompt.

---

## cd

Change default directory

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

### Description

The `cd` command changes the current working directory of the command prompt to the directory you specify. Using this command with the value `..` has the same effect as using the `up` command.

### Parameters

[<text>] - Valid CLI Directory

Use this parameter to specify the name of the directory to which you wish to change. If the directory name contains multiple parts, enclose the directory name in quotation marks (`"`).

### Examples

The following example changes the working directory of the CLI from the top directory to the `dashboard` directory. The command prompt displays the new working directory.

```
cluster1::> cd dashboard
cluster1::dashboard>
```

The following example changes the working directory from the top directory to the `storage aggregate` directory.

```
cluster1::> cd "storage aggregate"
cluster1::storage aggregate>
```

### See Also

`up`

---

## exit

Quit the CLI session

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

### Description

The `exit` command ends the current CLI session.

### Parameters

None

### Examples

The following example ends the current CLI session:

```
cluster1::> exit
Goodbye
```

## history

Show the history of commands for this CLI session

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

### Description

The `history` command displays the command history of the current CLI session. A numeric ID precedes each command. Use this number with the `redo` command to re-execute that history item.

### Parameters

None

### Examples

The following example displays the command history of the current CLI session:

```
cluster1::> history
  1  storage aggregate show
```

---

```
2 storage aggregate member show
3 set -privilege advanced
4 storage aggregate add-member -aggregate striped1 -flex-aggregate aggr12
5 storage aggregate add -aggregate striped1 -diskcount 14
6 storage aggregate show
7 volume show
```

## See Also

redo

---

## man

Display the online manual pages

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

### Description

The `man` command displays the manual page of the command you specify. If you do not specify a command, command displays the man page index.

### Parameters

[<text>] - Valid CLI command

The command for which you'd like to see the manual page. The syntax of the command is the same as the command itself. The `man` command supports abbreviations and tab completion of the command name.

### Examples

The following example displays the manual page for the storage aggregate create command.

```
cluster1::> man sto aggr cre
```

That example could also have been fully specified as:

```
cluster1::> man storage aggregate create
```

## redo

Execute a previous command

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

### Description

The `redo` command re-executes a command that has been executed previously in the current CLI session. Specify a previously run command using:

- 
- A string that matches part of a previous command. For example, if the only volume command you have run is `volume show`, enter `redo vol` to re-execute the command.
  - The numeric ID of a previous command, as listed by the `history` command. For example, enter `redo 4` to re-execute the fourth command in the history list.
  - A negative offset from the end of the history list. For example, enter `redo -2` to re-execute the command that you ran two commands ago.

## Parameters

[<text>] - String, Event Number, or Negative Offset

Use this parameter to specify a string, a numeric ID from the command history, or a negative number that identifies the command to be re-executed.

## Examples

The following example re-executes command number 10 in the command history:

```
cluster1::> redo 10
```

## See Also

`history`

---

## rows

Show/Set the rows for the CLI session

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

### Description

The `rows` command displays the number of rows that can be displayed in the current CLI session before the interface pauses output. If you do not set this value, it adjusts automatically based on the actual height of your terminal. If the actual height is undefined, the default number of rows is 24.

Specify a number to set the number of rows that can be displayed. Setting this value manually disables auto-adjustment. Specify zero (0) to disable pausing.

You can also set this value using the `set -rows` command.

### Parameters

[<integer>] - Number of Rows the Screen Can Display

Use this parameter to specify the number of rows your terminal can display.

### Examples

The following example displays the current number of rows, then resets the number of rows to 48:

```
cluster1::> rows
36
cluster1::> rows 48
```

### See Also

`set`



---

## set

Display/Set CLI session settings

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

### Description

The `set` command changes attributes of the user interface.

### Parameters

**[-privilege <PrivilegeLevel>]** - Privilege Level

Use this parameter to specify the privilege level of the command session. Possible values are

- `admin` - Used for routine system management commands
- `advanced` - Used for infrequent, dangerous, or complicated commands
- `diagnostic` - Used for detailed diagnostic commands that are used only by support personnel

**[-confirmations {on|off}]** - Confirmation Messages

Use this parameter with the value `on` to specify that the interface prompt for confirmation before executing potentially dangerous commands. Use this parameter with the value `off` to specify that the interface not prompt for confirmation, even before potentially dangerous commands execute. The default setting is `on`.

**[-showallfields {true|false}]** - Show All Fields

Use this parameter with the value `true` to specify that the interface display all field columns when displaying tabular output. Use this parameter with the value `false` to specify that the interface display only selected columns. The default setting is `false`.

**[-showseparator <text>]** - Show Separator

Use this parameter to specify the characters to use as the field separator. The field separator is used between field columns when `-showallfields` is set to `"true"`. The separator can be from one to three characters in length. When specifying the separator, enclose it in quotation marks ("). Set the separator to one or more spaces to disable this feature.

---

**[-active-help {true|false}]** - Active Help

Use this parameter with the value `true` to specify that pressing the question mark (?) key is sufficient to execute a help request. Use this parameter with the value `false` to specify that you must press the Return key after the question mark key to execute a help request. The default setting is `true`.

**[-units {auto|raw|B|KB|MB|GB|TB|PB}]** - Data Units

Use this parameter to specify the default units used when reporting data sizes. Possible values are:

- `auto` - Auto-scale data size for human-readable output
- `raw` - Bytes without unit designation
- `B` - Bytes
- `KB` - Kilobytes
- `MB` - Megabytes
- `GB` - Gigabytes
- `TB` - Terabytes
- `PB` - Petabytes

The default setting is `auto`.

**[-rows <integer>]** - Pagination Rows ('0' disables)

Use this parameter to specify the number of rows that can be displayed in the current CLI session before the interface pauses output. If you do not set this value, it adjusts automatically based on the actual height of your terminal. If the actual height is undefined, the default number of rows is 24.

Setting this value manually disables auto-adjustment. Specify zero (0) to disable pausing.

You can also set this value using the `rows` command.

**[-vserver <text>]** - Default Vserver

Use this parameter to specify the name of the Vserver to use as the default value for the `-vserver` parameter of commands.

**[-node <text>]** - Default Node

Use this parameter to specify the name of the node to use as the default value for the `-node` parameter of commands.

Use this parameter with the value `true` to specify that continuing commands should stop if they encounter an error. Use this parameter with the value `false` to specify that continuing commands should continue if they encounter an error.

The following example sets the privilege level to advanced.

The following examples cause all columns to be shown in output rows, with a comma used as the field separator.

## See Also

rows

---

## top

Go to the top-level directory

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

### Description

The `top` command changes the current working directory of the command prompt to the top-level command directory.

### Parameters

None

### Examples

The following example returns the command prompt from the `storage aggregate` directory to the top-level directory:

```
cluster1::storage aggregate> top
cluster1::>
```

### See Also

`storage aggregate`

---

## up

Go up one directory

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

### Description

The `up` command, which can also be specified as two dots (`..`), changes the current working directory of the command prompt to the directory that is up one level in the command hierarchy.

### Parameters

None

### Examples

The following example takes the command prompt up one level from the `storage aggregate` directory:

```
cluster1::storage aggregate> up
cluster1::storage>
```

### See Also

`storage aggregate`

---

## cluster create

Create a cluster

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

### Description

The `cluster create` command creates a cluster with one node. Once you create the cluster, add additional nodes to the cluster by using the `cluster join` command.

Cluster create enables you to manually create a cluster. Use the `cluster setup` command to use a wizard to create the cluster and join nodes to it.

Note that single-node clusters do not require configuring the cluster network. A cluster network interface must be configured before other nodes can join the cluster.

### Parameters

**-license** <License Code V2> - Base License

Use this parameter to specify the base license for the cluster. Obtain this value from your sales or support representative.

**-clustername** <text> - Cluster Name

Use this parameter to specify the name of the cluster you are creating. The cluster name must begin with a letter and cannot be more than 44 characters in length.

### Examples

The following example creates a cluster named `clus0`.

```
cluster1::> cluster create -license ABCDEFGHIJKLMN -clustername clus0
```

### See Also

`cluster join`   `cluster setup`

---

## cluster join

Join an existing cluster using the specified member's IP address

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

### Description

The `cluster join` command adds a node to an existing cluster. Use the `cluster create` command to create a cluster if one does not already exist.

Cluster join enables you to manually join a node to the cluster. Use the `cluster setup` command to use a wizard to join a node to the cluster.

Note that a cluster network interface must be configured for the cluster before other nodes can join the cluster.

### Parameters

**-clusteripaddr <IP Address>** - IP Address of a cluster interface from a node in the cluster

Use this parameter to specify the IP address of a cluster interface. This must be the IP address of a cluster interface of a node that is already in the cluster.

### Examples

The following example joins the local node to a cluster. The IP address 192.0.2.66 is the address of a cluster interface of a node that already belongs to the cluster.

```
cluster1::> cluster join -clusteripaddr 192.0.2.66
```

### See Also

`cluster create`   `cluster setup`

---

## cluster modify

Modify cluster node membership attributes

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

### Description

The `cluster modify` command modifies the cluster attributes of a node, including its eligibility to participate in the cluster.

At the advanced privilege level, you can use the command to specify whether a node holds epsilon. Epsilon is an extra fractional vote that enables quorum to form using slightly weaker requirements. For example, two out of four eligible nodes are sufficient to form quorum if one of those two nodes holds epsilon.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node to modify. If you do not specify a node, the command runs on the local node.

**[-epsilon** {true|false}] - Epsilon (privilege: advanced)

Use this parameter with the value `true` to specify that the node holds Epsilon in the cluster. Use this parameter with the value `false` to specify that the node does not hold Epsilon in the cluster. In a cluster, only one node can be designated as Epsilon at any given time. You can designate a node as Epsilon to add weight to its voting in a cluster with an even number of nodes.

**[-eligibility** {true|false}] - Eligibility

Use this parameter with the value `true` to specify that the node is eligible to participate in the cluster. Use this parameter with the value `false` to specify that the node is not eligible to participate in the cluster.

If you modify a node as ineligible to participate in the cluster, the command prompts you for confirmation before it runs.

### Examples

This example modifies a node to make it eligible to participate in the cluster.

```
cluster1::> cluster modify -node node3 -eligibility true
```



---

The following example removes epsilon from the node named node0 and adds it to the node named node1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
        when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
cluster1::*> cluster modify -node node0 -epsilon false
cluster1::*> cluster modify -node node1 -epsilon true
```

---

## cluster ping-cluster

Ping remote cluster interfaces and perform RPC server check

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

### Description

The `cluster ping-cluster` command probes network connectivity to remote cluster interfaces, and performs an RPC server check.

### Parameters

**-node** <nodename> - Node

Use this parameter to send the ping from the node you specify.

**[-use-sitelist {true|false}]** - Use Sitelist for Cluster Interfaces

Use this parameter with the value `true` to specify that the command use the sitelist to determine any incomplete cluster IP information. Use this parameter with the value `false` to specify that the command not use the sitelist.

**[-skip-rpccheck {true|false}]** - Skip RPC Server Check

Use this parameter with the value `true` to specify that the command not perform the `rpcinfo` check of remote hosts. Use this parameter with the value `false` to specify that the command perform the `rpcinfo` check. The `rpcinfo` check checks the status of the RPC servers on the remote hosts. By default, the `rpcinfo` check runs on the program number of the portmapper. Use the `-rpc-prognum` parameter to override this default.

**[-rpc-prognum <integer>]** - RPC Server to Check

Use this parameter to override default behavior and run the `rpcinfo` check on the program number you specify. By default, the `rpcinfo` check runs on the program number of the portmapper.

### Examples

The following example shows typical output for this command.

```
cluster1::*> cluster ping-cluster -node node1
Host is node1
Getting addresses from network interface table...
Local = 10.254.231.102  10.254.91.42
Remote = 10.254.42.25   10.254.16.228
Ping status:
Basic connectivity succeeds on 4 path(s)
```

---

```
Basic connectivity fails on 0 path(s)
Detected 1500 byte MTU on 4 path(s):
  Local 10.254.231.102 to Remote 10.254.16.228
  Local 10.254.231.102 to Remote 10.254.42.25
  Local 10.254.91.42 to Remote 10.254.16.228
  Local 10.254.91.42 to Remote 10.254.42.25
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

---

## cluster setup

Setup wizard

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

### Description

The `cluster setup` command runs the cluster setup wizard, which can be used to either create a cluster or join a node to an existing cluster. When you run the cluster setup wizard, enter the appropriate information at the prompts. You will be asked to provide the following information to create a cluster:

- Cluster name
- Cluster base license key
- Feature license keys
- Cluster administrator's password
- Cluster management interface port, IP address, netmask, default gateway
- Node management interface port, IP address, netmask, default gateway
- DNS domain names
- Name server IP addresses
- Location

You will be asked to provide the following information to join a cluster:

- Cluster name
- Node management interface port, IP address, netmask, default gateway

The cluster management interface is used for managing the cluster. It provides one IP address to manage the cluster and will fail over to another node, if necessary. This is the preferred IP address for managing the cluster, but you can also manage the cluster by logging in to the node management IP address of a node in the cluster. Since the cluster management interface must be able to fail over, the port role for the interface must be "data" and typically the best choice for an IP address is one on the data network. The node management interface will not fail over, so an IP address on the management network and a port with the role "node management" is the best choice. Alternatively, you can assign an IP address on the data network to the cluster management interface

---

- if that is better in your network topology - but the port must be a data port. The two examples below illustrate the cluster create and cluster join operations, respectively.

## Parameters

None

## Examples

The following example shows the create option of `cluster setup`.

```
node::> cluster setup
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
  Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

Do you want to create a new cluster or join an existing cluster? {create, join}:
create

Do you intend for this node to be used as a single node cluster? {yes, no} [no]:
no

System Defaults:
Private cluster network ports [e0a,e0b].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
The cluster will be connected without using network switches.

Do you want to use these defaults? {yes, no} [yes]:

It can take several minutes to create cluster interfaces...

Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.
Enter the cluster name: cluster1
Enter the cluster base license key: ABCDEFGHIJKLMNOP
Creating cluster cluster1
Starting cluster support services .....
Cluster cluster1 has been created.

Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.
Enter an additional license key []:

Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.
Enter the cluster administrator's (username "admin") password:
Retype the password:
Enter the cluster management interface port [e0c]:
Enter the cluster management interface IP address: 192.0.2.60
Enter the cluster management interface netmask: 255.255.255.192
Enter the cluster management interface default gateway: 192.0.2.1
```

---

A cluster management interface on port e0c with IP address 192.0.2.60 has been created. You can use this address to connect to and manage the cluster.

Enter the DNS domain names: data.example.com  
Enter the name server IP addresses: 192.0.2.147  
DNS lookup for the admin Vserver will use the data.example.com domain.

Step 4 of 5: Configure Storage Failover (SFO)  
You can type "back", "exit", or "help" at any question.

SFO is licensed.  
SFO will be enabled when the partner joins the cluster.

Step 5 of 5: Set Up the Node  
You can type "back", "exit", or "help" at any question.

Where is the controller located []: Sunnyvale  
Enter the node management interface port [e0c]: e0d  
Enter the node management interface IP address: 192.0.2.66  
Enter the node management interface netmask: 255.255.255.192  
Enter the node management interface default gateway: 192.0.2.1  
A node management interface on port e0d with IP address 192.0.2.66 has been created.

Cluster setup is now complete.

To begin storing and serving data on this cluster, log in to the command-line interface (for example, `ssh admin@192.0.2.60`) and complete the following additional tasks if they have not already been completed:

- Join additional nodes to the cluster by running "cluster setup" on those nodes.
- For HA configurations, verify that storage failover is enabled by running the "storage failover show" command.
- Create a Vserver by running the "vserver setup" command.

In addition to using the CLI to perform cluster management tasks, you can manage your cluster using OnCommand System Manager, which features a graphical user interface that simplifies many cluster management tasks. This software is available from the NetApp Support Site.

Exiting the cluster setup wizard.

**An example of using `cluster setup` to join a cluster is shown below.**

```
node::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:  
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value.

Do you want to create a new cluster or join an existing cluster? {create, join}:  
join

System Defaults:  
Private cluster network ports [e0a,e0b].  
Cluster port MTU values will be set to 9000.  
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]:

It can take several minutes to create cluster interfaces...

---

Step 1 of 3: Join an Existing Cluster

You can type "back", "exit", or "help" at any question.

Enter the name of the cluster you would like to join [cluster1]:

Joining cluster cluster1

Step 2 of 3: Configure Storage Failover (SFO)

You can type "back", "exit", or "help" at any question.

SFO is licensed.

SFO will be enabled when the partner joins the cluster.

Step 3 of 3: Set Up the Node

You can type "back", "exit", or "help" at any question.

Enter the node management interface port [e0c]:

Enter the node management interface IP address: 192.0.2.67

Enter the node management interface netmask [255.255.255.192]:

Enter the node management interface default gateway [192.0.2.1]:

A node management interface on port e0c with IP address 192.0.2.67 has been created.

Cluster setup is now complete.

To begin storing and serving data on this cluster, log in to the command-line interface (for example, `ssh admin@192.0.2.60`) and complete the following additional tasks if they have not already been completed:

- Join additional nodes to the cluster by running "cluster setup" on those nodes.
- For HA configurations, verify that storage failover is enabled by running the "storage failover show" command.
- Create a Vserver by running the "vserver setup" command.

In addition to using the CLI to perform cluster management tasks, you can manage your cluster using OnCommand System Manager, which features a graphical user interface that simplifies many cluster management tasks. This software is available from the NetApp Support Site.

Exiting the cluster setup wizard.

## See Also

`cluster create`   `cluster join`

---

## cluster show

Display cluster node members

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

### Description

The `cluster show` command displays information about the nodes in a cluster.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the nodes that match this parameter value.

[-**node-uuid** <UUID>] - UUID (privilege: advanced)

Selects the nodes that match this parameter value.

[-**epsilon** {true|false}] - Epsilon (privilege: advanced)

Selects the nodes that match this parameter value. In a cluster, only one node can be designated as Epsilon at any given time. You can designate a node as Epsilon to add weight to its voting in a cluster with an even number of nodes.

[-**eligibility** {true|false}] - Eligibility

Selects the nodes that match this parameter value (true means eligible to participate in the cluster).

[-**health** {true|false}] - Health

Selects the nodes that match this parameter value (true means online).

### Examples



---

The following example displays information about all nodes in the cluster:

```
cluster1::> cluster show
Node      Health  Eligibility
-----
node0     true    true
node1     true    true
node2     true    true
node3     true    true
```

The following example displays information about the node named node1:

```
cluster1::> cluster show -node node1
      Node: node1
Eligibility: true
      Health: true
```

## cluster unjoin

Unjoin or remove a node from the cluster

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

### Description

The `cluster unjoin` command removes a node from a cluster.

Before you can remove a node from a cluster, you must shut down all of the node's shared resources, such as virtual interfaces to clients. If any of a node's shared resources are still active, the command fails. The failure message will display which active resources must be shut down before the node can be removed from the cluster.

### Parameters

**-node** <nodename> - Node to Unjoin

Use this parameter to specify the name of the node to remove from the cluster.

### Examples

The following example shows how to remove the node named `node4` from the cluster.

```
cluster1::*> cluster unjoin -node node4
```

## cluster contact-info modify

Modify contact information for the cluster

---

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

## Description

The `cluster contact-info modify` command modifies contact information for the cluster administrators. If any values contain spaces, you must enclose those values in quotes.

Use the `cluster contact-info show` command to display contact information for the cluster administrators.

## Parameters

**[-primary-name <text>]** - Name of Primary Contact

Use this parameter to specify the name of the primary contact.

**[-primary-phone <text>]** - Phone Number of Primary Contact

Use this parameter to specify the phone number of the primary contact.

**[-primary-alt-phone <text>]** - Alternate Phone Number of Primary Contact

Use this parameter to specify the alternate phone number of the primary contact.

**[-primary-email <text>]** - Email Address or User ID of Primary Contact

Use this parameter to specify the email address of the primary contact.

**[-secondary-name <text>]** - Name of Secondary Contact

Use this parameter to specify the name of the secondary contact.

**[-secondary-phone <text>]** - Phone Number of Secondary Contact

Use this parameter to specify the phone number of the secondary contact.

**[-secondary-alt-phone <text>]** - Alternate Phone Number of Secondary Contact

Use this parameter to specify the alternate phone number of the secondary contact.

**[-secondary-email <text>]** - Email Address or User ID of Secondary Contact

Use this parameter to specify the email address of the secondary contact.

**[-business-name <text>]** - Business Name

Use this parameter to specify the name of the business responsible for this cluster.

**[-address <text>]** - Business Address

---

Use this parameter to specify the street address of the business responsible for this cluster.

**[-city <text>]** - City Where Business Resides

Use this parameter to specify the name of the city in which the business is located.

**[-state <text>]** - State Where Business Resides

Use this parameter to specify the name of the state or province in which the business is located.

**[-country <Country Code>]** - 2-Character Country Code

Use this parameter to specify the 2-character country code of the country in which the business is located.

**[-zip-code <text>]** - Postal Code Where Business Resides

Use this parameter to specify the postal or ZIP code area in which the business is located.

## Examples

The following example changes the name and phone numbers of the secondary contact person for the cluster.

```
cluster1::> cluster contact-info modify -secondary-name "John Doe" -secondary-  
phone 123.555.0156 -secondary-alt-phone 123.555.0178
```

The following example changes the mailing address of the business responsible for the cluster.

```
cluster1::> cluster contact-info modify -address "123 Example Avenue" -city  
Exampleville -state "New Example" -zip-code 99999 -country US
```

## See Also

cluster contact-info show

---

## cluster contact-info show

Display contact information for the cluster

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

### Description

The `cluster contact-info show` command displays contact information for the cluster administrators.

### Parameters

None

### Examples

The following example shows example output for this command.

```
cluster1::> cluster contact-info show
      Name of Primary Contact : Richard Roe
      Phone Number of Primary Contact : 123.555.0123
      Alternate Phone Number of Primary Contact : 123.555.0145
      Email Address or User Id of Primary Contact : roe@example.com
      Name of Secondary Contact : John Doe
      Phone Number of Secondary Contact : 123.555.0167
      Alternate Phone Number of Secondary Contact : 123.555.0189
      Email Address or User Id of Secondary Contact : doe@example.com
      Business Name : Example Dot Com
      Business Address : 123 Example Avenue
      City Where Business Resides : Exampleville
      State Where Business Resides : New Example
      2-Character Country Code : US
      Postal Code Where Business Resides : 99999
```

---

## cluster date modify

Modify the current date and time for the nodes in the cluster

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

### Description

The `cluster date modify` command sets the time zone, date, and time on every node in the cluster.

### Parameters

**[-timezone <Area/Location Timezone>]** - Time Zone

This parameter sets the timezone, specified in the Olson format.

**[-date {MM/DD/YYYY HH:MM:SS [{+|-}hh:mm]}]** - Date and Time

This parameter sets the date and time, in the format MM/DD/YYYY HH:MM:SS.

**[-dateandtime <[[[[cc]yy]mm]dd]hhmm[.ss]]>]** - Date and Time

This parameter sets the date and time information, in the format `[[[[cc]yy]mm]dd]hhmm[.ss]]`. The argument for setting the date and time is interpreted as follows:

- cc First 2 digits of the year (e.g., 20 for 2011).
- yy Last 2 digits of year (e.g., 10 for 2010).
- mm Numeric month, a number from 01 to 12.
- dd Day, a number from 01 to 31.
- hh Hour, a number from 00 to 23.
- mm Minute, a number from 00 to 59.
- ss Second, a number from 00 to 59.

If the first two digits of the year are omitted, and the last two digits are greater than 68, a date in the 1900s is used. Otherwise, a date in the 2000s is used. If all four digits of the year are omitted, the default is the current year. If the month or day is omitted, the default is the current month or day, respectively. If the seconds are omitted, the default

---

is set to 00. The system automatically handles the time changes for Daylight Saving and Standard time, and for leap seconds and years.

**[-utctimeandtime | -u <[[[[[cc]yy]mm]dd]hhmm[.ss]]>]** - UTC Date and Time

This parameter sets the date and time information in Coordinated Universal Time (UTC), in the format `[[[[[cc]yy]mm]dd]hhmm[.ss]]`. `-u` is an alias for `-utctimeandtime`. The argument for setting the date and time is interpreted as follows:

- cc First 2 digits of the year (e.g., 20 for 2011).
- yy Last 2 digits of year (e.g., 10 for 2010).
- mm Numeric month, a number from 01 to 12.
- dd Day, a number from 01 to 31.
- hh Hour, a number from 00 to 23.
- mm Minute, a number from 00 to 59.
- ss Second, a number from 00 to 59.

If the first two digits of the year are omitted, and the last two digits are greater than 68, a date in the 1900s is used. Otherwise, a date in the 2000s is used. If all four digits of the year are omitted, the default is the current year. If the month or day is omitted, the default is the current month or day, respectively. If the seconds are omitted, the default is set to 00. Time changes for Daylight Saving and Standard time, and for leap seconds and years, are handled automatically.

## Examples

The following example sets the date and time to January 1 2011, at 1:00 a.m.:

```
cluster1::> cluster date modify -date "01/01/2011 01:00:00"
```

The following example sets the date and time in the UTC format to May 22, 2011, at 09:25:00 a.m.:

```
cluster1::> cluster date modify -u 201105220925.00.
```

## cluster date show

Display the current date and time for the nodes in the cluster

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

---

## Description

The `cluster date show` command displays the time zone, date, and time settings for one or more nodes in the cluster. By default, the command displays date and time settings for all nodes in the cluster.

## Parameters

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

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

| [-utc ]

Displays date and time information in Coordinated Universal Time (UTC).

| [-utcdate ]

Displays date and time information in UTC.

| [-instance ] }

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

**[-node {<nodename>|local}]** - Node

Selects the nodes that match this parameter value.

**[-timezone <Area/Location Timezone>]** - Time Zone

Selects the nodes that match this parameter value (specified in the Olson format).

**[-date {MM/DD/YYYY HH:MM:SS [{+|-}hh:mm]}]** - Date and Time

Selects the nodes that match this parameter value.

**[-utc-date <MM/DD/YYYY HH:MM:SS>]** - UTC Date and Time

Selects the nodes that match this parameter value.

**[-dateandtime <[[[[cc]yy]mm]dd]hhmm[.ss]]>]** - Date and Time

Selects the nodes that match this parameter value (interpreted as follows):

- cc First 2 digits of the year (e.g., 20 for 2011).
- yy Last 2 digits of year (e.g., 11 for 2011).
- mm Numeric month, a number from 01 to 12.

- 
- dd Day, a number from 01 to 31.
  - hh Hour, a number from 00 to 23.
  - mm Minute, a number from 00 to 59.
  - ss Second, a number from 00 to 59.

**[-utcdateandtime | -u <[[[[[cc]yy]mm]dd]hhmm[.ss]]>]** - UTC Date and Time

-u is used as an alias for -utcdateandtime. Selects the nodes that match this parameter value (interpreted as follows):

- cc First 2 digits of the year (e.g., 20 for 2011).
- yy Last 2 digits of year (e.g., 11 for 2011).
- mm Numeric month, a number from 01 to 12.
- dd Day, a number from 01 to 31.
- hh Hour, a number from 00 to 23.
- mm Minute, a number from 00 to 59.
- ss Second, a number from 00 to 59.

## Examples

The following example displays the date and time settings for all nodes in the cluster:

```
cluster1::> cluster date show
Node      Date              Timezone
-----
node0     10/06/2011 09:35:15 America/New_York
node1     10/06/2011 09:35:15 America/New_York
node2     10/06/2011 09:35:15 America/New_York
node3     10/06/2011 09:35:15 America/New_York
4 entries were displayed.
```



---

## cluster ha modify

Modify high-availability configuration of cluster management services

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

### Description

The `cluster ha modify` command enables or disables cluster high availability in a two-node cluster. Enable high availability when performing some procedures, such as replacing hardware.

Note:

This command is required to enable high availability if the cluster only has two nodes. Do not run this command in a cluster that has three or more nodes.

Note:

Cluster high availability for two-node clusters differs from the storage failover technology used between two nodes for storage high availability.

### Parameters

**[-configured {true|false}]** - HA Configured

Use this parameter with the value `true` to enable high availability mode in the cluster. Use this parameter with the value `false` to disable high availability mode in the cluster.

### Examples

The following example enables cluster high availability in a cluster.

```
cluster::> cluster ha modify -configured true
```

## cluster ha show

Show high-availability configuration status for the cluster

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

---

## Description

The `cluster ha show` command displays the high-availability status of the cluster. Cluster high-availability mode applies only to two-node clusters.

## Parameters

None

## Examples

The following example displays the high-availability status for a two-node cluster:

```
cluster1::> cluster ha show
High Availability Configured: true
```

## cluster identity modify

Modify the cluster's attributes

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

## Description

The `cluster identity modify` command changes a cluster's identity information.

## Parameters

**[-name <text>]** - Cluster Name

Use this parameter to specify a new name for the cluster. The name of a cluster must begin with a letter, and cannot be more than 44 characters long.

**[-location <text>]** - Cluster Location

Use this parameter to specify the physical location of the cluster. For example, "Lab 5".

**[-contact <text>]** - Cluster Contact

Use this parameter to specify contact information for the cluster, such as a name or e-mail address.

## Examples

The following example renames the current cluster to `clus1`:

---

```
cluster1::> cluster identity modify -name clus1
```

## cluster identity show

Display the cluster's attributes including Name, Serial Number, Cluster UUID, Location and Contact

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

### Description

The `cluster identity show` command displays the identity information of the cluster.

### Parameters

None

### Examples

The following example displays the cluster's UUID, name, serial number, location and contact information:

```
cluster1::> cluster identity show
      Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
      Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
      Cluster Location: Lab2
      Cluster Contact: jsmith@example.com
cluster1::>
```

---

## cluster peer create

Create a new cluster peer relationship

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

### Description

The `cluster peer create` command establishes a peer relationship between two clusters. Cluster peering enables independent clusters to coordinate and exchange data.

Before creating a new cluster peer relationship, make sure that both clusters are individually healthy and that there are no other peer relationships between the two clusters that might interfere with the new relationship. Use the `cluster show` and `cluster peer show` commands on each cluster to display health, peering eligibility, and peering information about the two clusters.

### Parameters

**-peer-addr** <Remote InetAddress>, ... - Remote Intercluster Addresses

Use this parameter to specify the names or IP addresses of the logical interfaces used for intercluster communication. Separate the addresses with commas.

The addresses you provide here are associated with the remote cluster until you modify or delete the relationship, regardless of whether the addresses are valid. Make sure to provide addresses which you know will remain available on the remote cluster. You can use the hostnames of the remote cluster's intercluster addresses, the IP addresses of the remote cluster's intercluster LIFs or both.

**[-username <text>]** - Remote User Name

Use this parameter to specify a username that runs a reciprocal `cluster peer create` command on the peered cluster. If you choose not to use the reciprocal creation option, by not supplying a username for reciprocal creation, you must run `cluster peer create` again on the remote cluster to complete the peering relationship.

If you specify the username for the remote cluster, you will be prompted to enter the associated remote password. These credentials are not stored, they are used only during creation to authenticate with the remote cluster and to enable the remote cluster

---

to authorize the peering request. The provided username's profile must have access to the console application in the remote cluster.

Use the `security login role show` and `security login show` commands on each cluster to find user names and their privilege levels.

**[-timeout <integer>]** - Operation Timeout (seconds) (privilege: advanced)

Use this parameter to specify a timeout value for peer communications. Specify the value in seconds. The default timeout value is 60 seconds.

## Examples

This example creates a peer relationship between cluster1 and cluster2. This reciprocal create executes the create command on both the local cluster and the remote cluster. The cluster peer create command can use the hostnames of cluster2's intercluster addresses, the IP addresses of cluster2's intercluster LIFs or both. Note that the admin user's password was typed at the prompt, but was not displayed.

```
cluster1::> cluster peer create -peer-addr cluster2-d2,10.98.234.246 -username admin
```

Remote Password:

```
cluster1::> cluster peer show -instance
```

```
Peer Cluster Name: cluster2
Remote Intercluster Addresses: cluster2-d2, 10.98.234.246
Availability: Available
Remote Cluster Name: cluster2
Active IP Addresses: 10.98.234.246, 10.98.234.243
Cluster Serial Number: 1-80-123456
```

This example shows coordinated peer creation. The `cluster peer create` command was issued locally on each cluster. This does not require you to provide the username and password for the remote cluster. There is a password prompt, but if you are logged in as the admin user, you may simply press enter.

```
cluster1::> cluster peer create -peer-addr cluster2-d2, 10.98.234.246
```

Remote Password:

NOTICE: Addition of the local cluster information to the remote cluster has failed with the following error: not authorized for that command. You may need to repeat this command on the remote cluster.

```
cluster1::> cluster peer show
```

Peer Cluster Name	Cluster Serial Number	Availability
cluster2	1-80-123456	Available

```
cluster2::> cluster peer create -peer-addr cluster1-d2
```

Remote Password:

NOTICE: Addition of the local cluster information to the remote cluster has failed with the following error: not authorized for that command. You may need to repeat this command on the remote cluster.

```
cluster2::> cluster peer show
```

Peer Cluster Name	Cluster Serial Number	Availability
cluster1	1-80-123456	Available

---

## See Also

`security login role show` `security login show` `cluster show` `cluster peer show`

---

## cluster peer delete

Delete a cluster peer relationship

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

### Description

The `cluster peer delete` command removes a peering relationship. It removes the relationship records, state data, and all associated jobs.

Before removing the relationship, the command verifies that no resources depend on the relationship. For example, if any SnapMirror relationships exist, the command denies the request to delete the peering relationship. You must remove all dependencies for the deletion to succeed. The `cluster peer delete` command removes only the local instance of the peer relationship. An administrator in the peer cluster must use the `cluster peer delete` command there as well to completely remove the relationship.

### Parameters

**-cluster <text>** - Peer Cluster Name

Use this parameter to specify the peering relationship to delete by specifying the name of the peered cluster.

### Examples

This example shows a failed deletion due to a SnapMirror dependency.

```
cluster2::> cluster peer delete -cluster cluster1
Error: command failed: Unable to delete peer relationship. Reason: A
SnapMirror source exists in this cluster
```

---

## cluster peer modify

Modify cluster peer relationships

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

### Description

The `cluster peer modify` command modifies the attributes of a peering relationship. When you modify a peer relationship and specify `-peer-addr`s, all of the remote addresses must respond, must be intercluster addresses, and must belong to the remote cluster that is being modified; or the modification request is denied.

### Parameters

**-cluster** <text> - Peer Cluster Name

Use this parameter to specify the peering relationship to modify by specifying the name of the peered cluster.

**[-peer-addr**s <Remote InetAddress>, ...] - Remote Intercluster Addresses

Use this parameter to specify the names or IP addresses of the logical interfaces used for intercluster communication. Separate the addresses with commas. The list of addresses you provide replaces the existing list of addresses.

**[-timeout** <integer>] - Operation Timeout (seconds) (privilege: advanced)

Use this parameter to specify a timeout value for peer communications. Specify the value in seconds.

### Examples

This example modifies the peering relationship to use a new IP address in the remote cluster for intercluster communications.

```
cluster1::> cluster peer show -instance
      Peer Cluster Name: cluster2
Remote Intercluster Addresses: cluster2-d2, 10.98.234.246
      Availability: Available
      Remote Cluster Name: cluster2
      Active IP Addresses: 10.98.234.246, 10.98.234.243
      Cluster Serial Number: 1-80-123456

cluster1::> cluster peer modify -cluster cluster2 -peer-addr cluster2-
d2,10.98.234.264
```



---

## cluster peer ping

Initiate intercluster connectivity test

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

### Description

The `cluster peer ping` command displays the status of the network mesh used by the peering relationship. The command checks the network connection to each remote IP address known by the cluster. This includes all intercluster addresses. It is possible for a known address to be not present during the ping. These addresses are not checked, but the absence is temporary.

The most useful parameters for diagnosing problems are `-count` and `-packet-size`. Use the `-count` and `-packet-size` parameters to diagnose problems similarly to how you use them with the standard ping utility.

To display network connection status within a cluster, use the `network ping` command.

### Parameters

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

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

| **[-instance ]** }

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

**[-originating-node <nodename>|local]** - Node that Initiates Ping

Use this parameter to send the ping from the node you specify.

**[-destination-cluster <cluster\_name>]** - Cluster to Ping

Use this parameter to specify the peer cluster you wish to ping.

**[-destination-node <Peer Node Name>]** - Node to Ping in Destination Cluster

Use this parameter to specify a specific node in the destination cluster to ping.

---

**[-ip-address <IP Address>]** - Active IP Address

Use this parameter to specify the active IP address you wish to ping.

**[-count <integer>]** - Ping Count

Use this parameter to specify the number of requests to be sent to the destination.

**[-status {unknown\_node|internal\_error|unreachable|session\_reachable|interface\_reachable}]** - Status of Ping Operation

Use this parameter to display only ping results that have the status you specify.

**[-timeout <integer>]** - Ping Timeout in Seconds

Use this parameter to specify a timeout value in seconds for the ping operation.

**[-packet-size <integer>]** - Size of Packet

Use this parameter to specify the number of data bytes to be sent in the ping packet.

**[-ttl <integer>]** - Time to Live/ Number of Hops

Use this parameter to specify the maximum number of network hops a packet may make before it is considered a failure.

**[-response-time <double>]** - Response Time (ms)

Use this parameter to display only nodes that have the response time (in milliseconds) that you specify. This parameter is most useful when specified with a range of values, such as >500

## Examples

This example shows a ping of cluster1 and cluster2 from cluster2. All nodes are reachable.

```
cluster2::> cluster peer ping
Node: node1
Destination Node IP Address      Destination Count TTL RTT(ms) Status
-----
node1          10.98.228.230          1      255    0.209 interface_reachable
node2          10.98.228.234          1      255    0.42  interface_reachable
Node: node2
Destination Node IP Address      Destination Count TTL RTT(ms) Status
-----
node1          10.98.228.230          1      255    0.358 interface_reachable
node2          10.98.228.234          1      255    0.17  interface_reachable
Node: node1
Destination Node IP Address      Destination Count TTL RTT(ms) Status
-----
node3          10.98.229.22           1      255    0.336 interface_reachable
node4          10.98.229.29           1      255    0.354 interface_reachable
Node: node2
Destination Node IP Address      Destination Count TTL RTT(ms) Status
-----
node3          10.98.229.22           1      255    0.354 interface_reachable
node4          10.98.229.29           1      255    0.336 interface_reachable
6 entries were displayed.
```

---

## See Also

network ping

---

## cluster peer show

Display peer cluster information

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

### Description

The `cluster peer show` command displays information about the peering relationships between the current cluster and other clusters. Cluster peering enables independent clusters to coordinate and exchange data.

### Parameters

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

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

| [-**instance** ] }

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

[-**cluster** <text>] - Peer Cluster Name

Selects the peered clusters that match this parameter value.

[-**cluster-uuid** <UUID>] - Cluster UUID (privilege: advanced)

Selects the peered clusters that match this parameter value.

[-**peer-addrs** <Remote InetAddress>, ...] - Remote Intercluster Addresses

Selects the peered clusters that match this parameter value (remote-host name or IP address).

[-**availability** {available|unavailable}] - Availability

Selects the peered clusters that match this parameter value.

[-**rcluster** <text>] - Remote Cluster Name

Selects the peered clusters that match this parameter value.

[-**ip-addrs** <Remote InetAddress>, ...] - Active IP Addresses

---

Selects the peered clusters that match this parameter value.

**[-serialnumber <Cluster Serial Number>]** - Cluster Serial Number

Selects the peered clusters that match this parameter value.

**[-timeout <integer>]** - Operation Timeout (seconds) (privilege: advanced)

Selects the peered clusters that match this parameter value.

## Examples

This example displays the name and serial number of a peered cluster, along with its connection availability.

```
cluster1::> cluster peer show
Peer Cluster Name      Cluster Serial Number  Availability
-----
cluster2               1-80-123456           Available
```

This example displays detailed information about the peering relationship.

```
cluster1::> cluster peer show -instance
Peer Cluster Name: cluster2
Remote Intercluster Addresses: cluster2-d2, 10.98.234.246
Availability: Available
Remote Cluster Name: cluster2
Active IP Addresses: 10.98.234.246, 10.98.234.243
Cluster Serial Number: 1-80-123456
```

---

## cluster peer health show

Check peer cluster health

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

### Description

The `cluster peer health show` command displays information about the health of the nodes in peer clusters from the perspective of the nodes in the local cluster. The command obtains health information by performing connectivity and status probes of each peer cluster's nodes from each node in the local cluster.

To enable quick access to remote cluster health information, remote cluster health status is periodically checked and cached. These cached results enable users and system features to quickly assess the availability of remote resources. By default, this command accesses cached results. Use the `-bypass-cache true` option to force a current, non-cached check of remote cluster health.

### Parameters

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

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

| [-instance ] }

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

**[-originating-node {<nodename>|local}]** - Local Node

Selects the node that matches this parameter value.

**[-destination-cluster <cluster\_name>]** - Peer Cluster

Selects the cluster that matches this parameter value.

**[-destination-node <Peer Node Name>]** - Peer Node

Selects the node that matches this parameter value.

**[-destination-cluster-uuid <UUID>]** - Peer UUID

---

Selects the cluster that matches this parameter value.

**[-data-ping {unknown\_node|internal\_error|unreachable|session\_reachable|interface\_reachable}]** - Status of Data Ping Operation

Selects the nodes that match this parameter value.

**[-icmp-ping {unknown\_node|internal\_error|unreachable|session\_reachable|interface\_reachable}]** - Status of ICMP Ping Operation

Selects the nodes that match this parameter value.

**[-node-health {true|false}]** - RDB Health of the Node

Selects the nodes that match this parameter value (`true` means healthy).

**[-cluster-health {true|false}]** - Cluster Health

Selects the nodes that match this parameter value (`true` means healthy).

**[-availability {true|false}]** - Communication Indicator

Selects the nodes that match this parameter value (`true` means communicating).

**[-bypass-cache {true|false}]** - Bypass Cache and Determine Health

Bypasses cached results to determine current cluster health (`true` means bypass the cache). Cached results may not be current, but they are displayed more quickly.

## Examples

The following example shows typical output for this command in a cluster of two nodes that has a peer cluster of two nodes.

```
cluster1::> cluster peer health show
Node      Cluster-Name  Node-Name  RDB-Health  Cluster-Health  Availability
-----
node1
  cluster2
    Data: interface_reachable  node3  true        true        true
    ICMP: interface_reachable  node4  true        true        true
  Data: interface_reachable
  ICMP: interface_reachable
node2
  cluster2
    Data: interface_reachable  node3  true        true        true
    ICMP: interface_reachable  node4  true        true        true
  Data: interface_reachable
  ICMP: interface_reachable
4 entries were displayed.
```

The following example shows detailed health information for node3 in cluster2 from the perspective of node1 in cluster1.

```
cluster1::> cluster peer health show -originating-node node1 -destination-cluster
cluster2 -destination-node node3 -instance
Local Node: node1
```

---

```
Peer Cluster: cluster2
Peer Node: node3
Peer UUID: 5e4befb2-1f36-11d0-98c9-123476563412
Status of Data Ping Operation: interface_reachable
Status of ICMP Ping Operation: interface_reachable
RDB health of the node: true
Cluster Health: true
Communication Indicator: true
```



---

## cluster peer job delete

Delete a job

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

### Description

The `cluster peer job delete` command deletes a job from a peered cluster. The command does not stop a job if it is currently running. Use the `cluster peer job stop` command to stop a job that is currently running. Use the `cluster peer job show` command to view a list of jobs that can be deleted.

### Parameters

**-cluster** <cluster\_name> - Cluster Name

Use this parameter to specify the name of the peered cluster in which the job runs.

**-id** <integer> - Job ID

The numeric ID of the job you want to delete. A job ID is a positive integer.

### Examples

The following example deletes the job in cluster2 that has ID 99:

```
cluster1::> cluster peer job delete -cluster cluster2 -id 99
```

### See Also

`cluster peer job stop`   `cluster peer job show`

---

## cluster peer job pause

Pause a job

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

### Description

The `cluster peer job pause` command pauses a job that is running on a peered cluster. Use the `cluster peer job resume` command to resume a paused job. Use the `cluster peer job show` command to view a list of running jobs that can be paused.

### Parameters

**-cluster** <cluster\_name> - Cluster Name

Use this parameter to specify the name of the peered cluster in which the job runs.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the job to pause.

### Examples

The following example pauses the job running on cluster2 that has ID 183:

```
cluster1::> cluster peer job pause -cluster cluster2 -id 183
```

### See Also

`cluster peer job resume`   `cluster peer job show`

---

## cluster peer job resume

Resume a job

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

### Description

The `cluster peer job resume` command resumes a job that was previously paused by using the `cluster peer job pause` command. Use the `cluster peer job show` command to view a list of paused jobs that can be resumed.

### Parameters

**-cluster** <cluster\_name> - Cluster Name

Use this parameter to specify the name of the peered cluster in which the job runs.

**-id** <integer> - Job ID

The numeric ID of the paused job to be resumed. A job ID is a positive integer.

### Examples

The following example resumes the paused job in cluster2 that has ID 183:

```
cluster2::> cluster peer job resume -cluster cluster2 -id 183
```

### See Also

`cluster peer job pause`   `cluster peer job show`

---

## cluster peer job show

Display a list of jobs in a cluster

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

### Description

The `cluster peer job show` command displays information about jobs running in peer clusters. By default, the command displays information about all current jobs in the local cluster.

To display detailed information about a specific job, run the command with the `-cluster` and `-id` parameters.

### Parameters

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

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

| **[-inprogress]** ]

Displays the job ID, the job name, the owning Vserver, and the progress of the job.

| **[-jobstate]** ]

Displays information about each job's state, including the queue state, whether the job was restarted, and when the job has completely timed out.

| **[-jobuuid]** ]

Displays the job ID, the job name, the owning Vserver, and the job UUID.

| **[-times]** ]

Displays the job ID, the job name, the owning Vserver, the time when the job was last queued, the time when the job was last started, and the time when the job most recently ended.

| **[-type]** ]

Displays the job ID, the job name, the job type, and the job category.

| **[-instance]** }

---

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

**[-cluster <cluster\_name>]** - Cluster Name

Selects the jobs that match this parameter value.

**[-id <integer>]** - Job ID

Selects the jobs that match this parameter value.

**[-name <text>]** - Name

Selects the jobs that match this parameter value.

**[-description <text>]** - Description

Selects the jobs that match this parameter value.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Selects the jobs that match this parameter value.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Selects the jobs that match this parameter value.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Selects the jobs that match this parameter value.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Selects the jobs that match this parameter value.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Selects the jobs that match this parameter value.

**[-restarted {true|false}]** - Restarted?

Selects the jobs that match this parameter value.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Selects the jobs that match this parameter value. Supported job state values are:

- Initial - job has been created but not queued yet
- Queued - job is in the queue; it could be ready to run immediately or it may be scheduled to run at a later time
- Running - the job has been picked by an instance of the Job Manager and is running

- 
- Waiting - the job is waiting for another job to complete
  - Pausing - the job is in the process of pausing after being requested to pause
  - Paused - the job is indefinitely paused
  - Quitting - the job has been requested to terminate and it is shutting down
  - Success - the job has successfully completed and the results are available
  - Failure - the job has failed
  - Reschedule - the job is being re-scheduled
  - Error - internal error occurred
  - Quit - the job has been requested to terminate
  - Dead - the job exceeded the drop dead time and is being removed from the queue
  - Unknown - the state of the job is unknown
  - Restart - the job is restartable
  - Dormant - the job is inactive while waiting on some external event

**[-code <integer>]** - Status Code

Selects the jobs that match this parameter value.

**[-completion <text>]** - Completion String

Selects the jobs that match this parameter value.

**[-jobtype <text>]** - Job Type

Selects the jobs that match this parameter value.

**[-category <text>]** - Job Category

Selects the jobs that match this parameter value.

**[-uuid <UUID>]** - UUID (privilege: advanced)

Selects the jobs that match this parameter value.

**[-progress <text>]** - Execution Progress

Selects the jobs that match this parameter value.

## Examples

The following example displays information about all the jobs running in cluster2:

```
cluster1::> cluster peer job show -cluster cluster2
Job ID      Name      State      Description
```

```

-----
Cluster: cluster2
1      Certificate Expiry Check
      Queued      Certificate Expiry Check
2      Licensing      Queued      License Checking
3      CLUSTER BACKUP AUTO 8hour
      Running      Cluster Backup Job
4      CLUSTER BACKUP AUTO daily
      Queued      Cluster Backup Job
5      CLUSTER BACKUP AUTO weekly
      Queued      Cluster Backup Job
10     Vol Reaper      Queued      Vol Reaper Job
349    Peer Manager for cluster cluster3
      Queued      Cluster Peer Manager Job for cluster
      cluster3
427    Peer Manager for cluster cluster1
      Queued      Cluster Peer Manager Job for cluster
      cluster1
10 entries were displayed.

```

---

## cluster peer job stop

Stop a job

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

### Description

The `cluster peer job stop` command stops jobs that are running in peer clusters. The command signals the job to quit. A stopped job cannot be resumed. Use the `cluster peer job delete` command to remove a job from the job queue. Use the `cluster peer job pause` command to pause a job so that you can later resume it. Use the `cluster peer job show` command to view a list of jobs that are running in peer clusters.

### Parameters

**-cluster** <cluster\_name> - Cluster Name

Use this parameter to specify the name of the peered cluster in which the job runs.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the job to stop. A job ID is a positive integer.

### Examples

The following example stops the job running on cluster2 that has ID 101:

```
cluster2::> cluster peer job stop -cluster cluster2 -id 101
```

### See Also

`cluster peer job delete`   `cluster peer job pause`   `cluster peer job show`



---

## cluster peer job watch-progress

Watch the progress of a job

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

### Description

The `cluster peer job watch-progress` command displays the progress of jobs running in peer clusters, and updates that display periodically. You can specify the frequency of the updates. To stop watching the job, press ctrl-C.

### Parameters

**-cluster** <cluster\_name> - Cluster Name

Use this parameter to specify the name of the peered cluster in which the job runs.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the job whose progress you will monitor.

**[-interval <integer>]** - Refresh Interval (seconds)

Use this parameter to specify the number of seconds between display updates.

### Examples

The following example monitors the progress of the job that has ID 222, that is running on cluster2. The progress is updated every 3 seconds.

```
cluster1::> cluster peer job watch-progress -cluster cluster2 -id 222 -interval 3
```

## cluster ring show

Display cluster node member's replication rings

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

### Description

The `cluster ring show` command displays a cluster's ring-replication status. Support personnel might ask you to run this command to assist with troubleshooting.

---

## Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the rings that match this parameter value.

[-**unitname** {mgmt|vldb|vifmgr|bcomd}] - Unit Name

Selects the rings that match this parameter value. Possible values are:

- `mgmt` - The management application
- `vldb` - The volume location database
- `vifmgr` - The virtual-interface manager
- `bcomd` - The SAN management daemon

[-**online** {master|secondary|offline}] - Status

Selects the rings that match this parameter value.

[-**epoch** <integer>] - Epoch

Selects the rings that match this parameter value.

[-**master** <nodename>] - Master Node

Selects the rings that match this parameter value.

[-**local** <nodename>] - Local Node

Selects the rings that match this parameter value.

[-**db-epoch** <integer>] - DB Epoch

Selects the rings that match this parameter value.

[-**db-trnxs** <integer>] - DB Transaction

Selects the rings that match this parameter value.

---

**[-num-online <integer>]** - Number Online

Selects the rings that match this parameter value.

**[-rdb-uuid <UUID>]** - RDB UUID

Selects the rings that match this parameter value.

## Examples

The following example displays information about all replication rings in a two-node cluster:

```
cluster1::*> cluster ring show
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0     mgmt      1              1          1068   node0     master
node0     vldb      1              1           98   node0     master
node0     vifmgr    1              1          350   node0     master
node0     bcmd      1              1           56   node0     master
node1     mgmt      1              1          1068   node0     secondary
node1     vldb      1              1           98   node0     secondary
node1     vifmgr    1              1          350   node0     secondary
node1     bcmd      1              1           56   node0     secondary
8 entries were displayed.
```

---

## cluster statistics show

Display cluster-wide statistics

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

### Description

The `cluster statistics show` command displays the following information. Each item lists the current value and; if applicable, the change (delta) from the previous reported value.

- CPU busy percentage
- Average of CPU busy percentage (advanced privilege level only)
- Total number of NFS and CIFS operations
- Number of NFS operations
- Number of CIFS operations
- Number of cache operations (advanced privilege level only)
- Total amount of network data received (advanced privilege level only)
- Total amount of network data sent (advanced privilege level only)
- Number of packets received (advanced privilege level only)
- Number of packets sent (advanced privilege level only)
- Busy percentage for the data network
- Amount of data received on the data network
- Amount of data sent on the data network
- Busy percentage for the cluster network
- Amount of data received on the cluster network
- Amount of data sent on the cluster network
- Amount of data read from disk
- Amount of data written to disk

At the diagnostic privilege level, the command displays the following information:

- Average of CPU busy percentage
- CPU busy percentage
- Total number of operations
- Number of NFS operations
- Number of CIFS operations
- Number of Fcache operations
- Number of SpinFS operations
- Total amount of network traffic received
- Total amount of network traffic sent
- Percentage of data-network utilization
- Amount of data-network traffic received
- Amount of data-network traffic sent
- Percentage of cluster-network utilization
- Amount of cluster-network traffic received
- Amount of cluster-network traffic sent
- Amount of data read from disk
- Amount of data written to disk
- Number of packets received
- Number of packets sent

**Parameters**

None

**Examples**

The following example displays cluster statistics:

```
cluster1::> cluster statistics show
Counter      Value      Delta
-----
CPU Busy:    84%      +27
Operations:
  Total:     951471448  7210/s:11s
  NFS:      12957951479 13759/s:11s
  CIFS:      342195460   230/s:11s
Data Network:
  Busy:      0%      -
  Received:  1.98TB    3.18MB/s:11s
  Sent:      6.20TB    903KB/s:11s
Cluster Network:
```

---

Busy:	0%	-
Received:	6.33TB	1.34MB/s:11s
Sent:	6.24TB	3.54MB/s:11s
Storage Disk:		
Read:	207TB	82.7MB/s:11s
Write:	53.3TB	53.5MB/s:11s

---

## dashboard alarm show

Display current over-threshold alarms

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

### Description

The `dashboard alarm show` command displays information about over-threshold alarms. Over-threshold alarms are generated when a value exceeds the configured threshold.

### Parameters

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

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

| [-instance ] }

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

[-type <Metric Type>] - Metric Type

Use this parameter to display information only about alarms with the object type you specify, such as `cpu-busy`, `port-util`, `op-latency`, or `aggregate-used`.

[-node {<nodename>|local}] - Node

Selects the alarms that match this parameter value.

[-name <text>] - Object Name

Selects the alarms that match this parameter value (such as an aggregate named `aggr0`).

[-state <Alarm Monitoring State>] - Alarm State

Selects the alarms that match this parameter value. Possible states are `ok`, `warning`, and `critical`. States are displayed according to the configured thresholds. Use the `dashboard alarm thresholds modify` command to configure alarm thresholds.

[-ems-state <EMS State>] - EMS State

---

Selects the alarms that match this parameter value. Possible states are `rising` and `falling`.

**[-value <Counter>]** - Last Value

Selects the alarms that match this parameter value.

**[-high-value <Counter>]** - High Value

Selects the alarms that match this parameter value. This parameter is most useful when used with a range, such as `>90%`.

## Examples

The following example shows the default alarm dashboard output when an alarm exceeds its threshold:

```
cluster1::> dashboard alarm show
ObjectType      Node      Name      State      LastValue      HighValue
-----
aggregate-used  node1    aggr0     critical   57%            57%
```

## See Also

`dashboard alarm thresholds modify`



---

## dashboard alarm thresholds modify

Modify alarm thresholds

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

### Description

The `dashboard alarm thresholds modify` command modifies the cluster-wide configuration of alarm thresholds.

### Parameters

**-type** <Metric Type> - Metric Type

Use this parameter to specify the type of object to monitor, such as `cpu-busy`, `port-util`, `op-latency`, `port-problems`, or `aggregate-used`.

**[-warning** <Counter>] - Warning Threshold

Use this parameter to specify the threshold value that generates a warning alarm for an event.

**[-critical** <Counter>] - Critical Threshold

Use this parameter to specify the threshold value that generates a critical alarm for an event.

**[-send-ems** {true|false}] - Send EMS

Use this parameter with the value `true` to specify that an EMS (Event Management System) message is sent when the alarm is generated or cleared. Use this parameter with the value `false` to specify that an EMS message is not sent.

**[-interval** <integer>] - Interval (secs)

Use this parameter to specify the interval in seconds at which the alarm dashboard monitors objects. Valid values are between 60 and 6,000 seconds.

### Examples

The following example modifies the warning and critical alarm thresholds for space used on aggregates. When 50% of the aggregate's space is consumed, a warning message is generated. When 60% of the aggregate's space is consumed, a critical message is generated. EMS messages are sent both when the value rises to the critical threshold,

---

and when it subsequently falls to the warning threshold. The system checks values every 5 minutes.

```
cluster1::> dashboard alarm thresholds modify -type aggregate-used -warning 50 -critical 60 -send-ems true -interval 300
```

## dashboard alarm thresholds show

Display alarm thresholds

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

### Description

The `dashboard alarm thresholds show` command displays information about alarm thresholds.

### Parameters

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

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

| **[-instance ]** }

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

**[-type <Metric Type>]** - Metric Type

Selects the alarms that match this parameter value.

**[-warning <Counter>]** - Warning Threshold

Selects the alarms that match this parameter value.

**[-critical <Counter>]** - Critical Threshold

Selects the alarms that match this parameter value.

**[-send-ems {true|false}]** - Send EMS

Selects the alarms that match this parameter value.

**[-interval <integer>]** - Interval (secs)

Selects the alarms that match this parameter value.

---

**[-critical-ems <text>]** - Critical EMS

Selects the alarms that match this parameter value.

**[-normal-ems <text>]** - Normal EMS

Selects the alarms that match this parameter value. The normal EMS message is sent when a value returns to the warning threshold after having reached the critical threshold.

## Examples

The following example shows the default dashboard alarm threshold information:

```
cluster1::> dashboard alarm thresholds show
-----Thresholds-----
ObjectType      Warning    Critical    SendEMS
-----
cpu-busy         100%      -           false
port-util        100%      -           false
op-latency       100ms     500ms      false
aggregate-used   85%       95%        true
port-problems    1%        5%         false
```

---

## dashboard health vservers show-aggregate

Display Vserver aggregate issues

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

### Description

The `dashboard health vservers show-aggregate` command displays information about aggregate health.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-**aggregate** <aggregate name>] - Aggregate

Use this parameter to display health information only about the aggregate you specify.

[-**time** <MM/DD HH:MM:SS>] - Time

Use this parameter to display information only about health issues occurring at the date and time you specify.

[-**node** {<nodename>|local}] - Node

Use this parameter to display health information only about the node you specify.

[-**severity** {ok|info|warning|critical}] - Severity

Use this parameter to display information about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

[-**description** <text>] - Description

Use this parameter to display information only about health issues whose descriptions match the text you specify.

### Examples

The following example shows health information for all aggregates in the cluster:

```
cluster1::> dashboard health vserver show-aggregate
Vserver      Aggregate  Time           Node    Severity
-----
vs0          aggr1      4/9 17:08:16   node1   warning
mgmtgwd.aggregate-used.rising: Percentage used on
aggregate aggr1 has a value of 95.
vs0          aggr2      4/9 17:08:51   node1   warning
mgmtgwd.aggregate-used.rising: Percentage used on
aggregate aggr2 has a value of 98.
vs1          aggr1      4/6 16:03:53   node2   warning
mgmtgwd.aggregate-used.rising: Percentage used on
aggregate aggr1 has a value of 90.
vs1          aggr2      4/6 16:03:53   node2   warning
mgmtgwd.aggregate-used.rising: Percentage used on
aggregate aggr2 has a value of 90.
4 entries were displayed.
```

---

## dashboard health vservers show-combined

Display all aggregate, LIF, port, protocol or volume issues

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

### Description

The `dashboard health vservers show-combined` command displays the health status of aggregates, LIFs, ports, protocols, and volumes in Vservers.

### Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-category <Health Categories>] - Health Issue Type

Use this parameter to display health information only about health issues in the category you specify, such as `protocol`, `lif`, `volume`, `port`, or `aggregate`.

[-objectname <text>] - Object Name

Use this parameter to display health information only about the object you specify, such as the name of a node.

[-time <MM/DD HH:MM:SS>] - Time

Use this parameter to display health information only about issues occurring at the date and time you specify.

[-node {<nodename>|local}] - Issuing Node

Use this parameter to display health information only about the node you specify.

---

**[-event <text>]** - Event name

Use this parameter to display health information only about the event you specify.

**[-severity {ok|info|warning|critical}]** - Severity

Use this parameter to display information only about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

**[-description <text>]** - Description

Use this parameter to display information only about health issues whose descriptions match the text you specify.

## Examples

The following example shows Vserver health information:

```
cluster1::> dashboard health vsriver show-combined
Vserver      Category Object Name Time          Severity
-----
vs0          lif      datalif1  4/12 11:30:13 critical
lifmgr.lifdown.noports: LIF datalif1 (on Vserver vs0),
IP address 192.0.2.132, currently cannot be hosted
on node node1, port e0d, or anywhere else, and is
being marked as down.

vs0          volume   root_vs0  4/6  15:57:00 warning
waf1.vvol.offline: Volume
'root_vs0@vserver:67a42b95-e454-11db-80e8-000423b7394e'
has been set temporarily offline

vs0          volume   vol0      4/6  12:53:22 warning
waf1.vol.full: file system on volume datalif1vol0@
vserver:67a42b95-e454-11db-80e8-000423b7394e is full

vs0          volume   vol1      4/6  12:53:24 warning
waf1.vvol.offline: Volume
'vol1@vserver:67a42b95-e454-11db-80e8-000423b7394e'
has been set temporarily offline

vs0          volume   vol2      4/6  12:53:26 warning
waf1.vvol.offline: Volume
'vol2@vserver:67a42b95-e454-11db-80e8-000423b7394e'
has been set temporarily offline
5 entries were displayed.
```

---

## dashboard health vservers show-lif

Display Vserver lif issues

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

### Description

The `dashboard health vservers show-lif` command displays information about the health of logical interfaces (LIFs).

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-**lif** <lif-name>] - Logical Interface

Use this parameter to display health information only about the LIF you specify.

[-**time** <MM/DD HH:MM:SS>] - Time

Use this parameter to display health information only about health issues that occurred at the date and time you specify.

[-**node** {<nodename>|local}] - Node

Use this parameter to display health information only about the node you specify.

[-**severity** {ok|info|warning|critical}] - Severity

Use this parameter to display information only about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

[-**description** <text>] - Description



---

Use this parameter to display information only about health issues whose descriptions match the text you specify.

## Examples

The following example shows health information for a Vserver on which all logical interfaces are working properly:

```
cluster1::> dashboard.health vservers show-lif
There are no logical interface issues.
```

## dashboard health vservers show-port

Display Vserver port issues

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

## Description

The `dashboard health vservers show-port` command displays information about port health.

## Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-node {<nodename>|local}] - Node

Use this parameter to display health information only about the node you specify.

[-port <text>] - Port

Use this parameter to display health information only about the network port you specify.

[-time <MM/DD HH:MM:SS>] - Time

---

Use this parameter to display health information only about issues occurring at the date and time you specify.

**[-severity {ok|info|warning|critical}]** - Severity

Use this parameter to display information only about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

**[-description <text>]** - Description

Use this parameter to display information only about health issues whose descriptions match the text you specify.

## Examples

The following example shows health information for all network ports in the cluster that have a health issue:

```
cluster1::> dashboard health vserver show-port
Vserver      Node    Port    Time              Severity
-----
vs1          node3   e0d     3/22 01:43:00    warning
               vifmgr.portdown: A link down event was
               received on node node3, port e0d.
```

---

## dashboard health vservers show-protocol

Display Vserver protocol issues

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

### Description

The `dashboard health vservers show-protocol` command displays information about protocol health.

### Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-component-type <component type>] - Component Type

Use this parameter to display health information only about the component type you specify.

[-component-name <text>] - Component Name

Use this parameter to display health information only about the component name you specify.

[-time <MM/DD HH:MM:SS>] - Time

Use this parameter to display health information only about issues occurring at the date and time you specify.

[-node {<nodename>|local}] - Node

Use this parameter to display health information only about the node you specify.

---

**[-severity {ok|info|warning|critical}]** - Severity

Use this parameter to display information only about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

**[-description <text>]** - Description

Use this parameter to display information only about health issues whose descriptions match the text you specify.

## Examples

The following example shows health dashboard information for a cluster in which all protocols are working properly:

```
cluster1::> dashboard health vserver show-protocol
There are no protocol issues.
```

The following example shows health information about a Vserver on which there are two warnings about protocols:

```
cluster1::> dashboard health vserver show-protocol -vserver vs0
Component Component
Vserver Type Name Time Node Severity
-----
vs0 CIFSSERV cifsserv0 3/21 14:13:54 node1 warning
mgmt.cifsserver.failure: Failed to configure CIFS
server.
vs0 CIFSSHARE cifshome 3/21 14:16:04 node1 warning
mgmt.cifsshare.failure: Failed to configure CIFS
share.
2 entries were displayed.
```

---

## dashboard health vservers show-volume

Display Vserver volume issues

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

### Description

The `dashboard health vservers show-volume` command displays health information about volumes.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Use this parameter to display health information only about the Vserver you specify.

[-**volume** <volume name>] - Volume

Use this parameter to display health information only about the volume you specify.

[-**time** <MM/DD HH:MM:SS>] - Time

Use this parameter to display health information only about issues occurring at the date and time you specify.

[-**node** {<nodename>|local}] - Node

Use this parameter to display health information only about the node you specify.

[-**severity** {ok|info|warning|critical}] - Severity

Use this parameter to display information only about health issues that have the severity you specify. Possible values for this parameter are `ok`, `warning`, and `critical`.

[-**description** <text>] - Description

---

Use this parameter to display information only about health issues whose descriptions match the text you specify.

### Examples

The following example shows health information about volumes named vol0 and root\_vs0 on node1:

```
cluster1::> dashboard health vsserver show-volume -volume vol0,root_vs0 -node
node1
Vserver          Volume      Time           Node    Severity
-----
vs0              vol0        3/12 12:10:17  node1   warning
    waf1.vvol.offline: Volume
    'vol0@vsserver:f18b00c4-d0b0-11db-891f-423b6f0a2'
    has been set temporarily offline
vs0              root_vs0    3/12 12:11:43  node1   warning
    waf1.vvol.offline: Volume
    'root_vs0@vsserver:f18b00c4-d0b0-11db-891f-423b6f0a2'
    has been set temporarily offline
2 entries were displayed.
```

---

## dashboard health vservers show

Display Vserver health dashboard

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

### Description

The `dashboard health vservers show` command displays information about Vserver health. This information includes current operational state and status, critical alerts, warnings, informational messages, and comments.

### Parameters

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

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

| [-instance ] }

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

**[-vservers <vservers name>]** - Vserver Name

Selects the items that match this parameter value.

**[-vstatus {online|offline}]** - Status

Selects the items that match this parameter value.

**[-vhealth {ok|info|warning|critical}]** - Health

Selects the items that match this parameter value.

**[-critical <integer>]** - Critical Issues

Selects the items that match this parameter value.

**[-warning <integer>]** - Warning Issues

Selects the items that match this parameter value.

**[-informational <integer>]** - Informational Issues

Selects the items that match this parameter value.

---

**[-nfs-config-status {configured|notconfigured|disabled}]** - NFS Configuration Status

Selects the items that match this parameter value.

**[-nfs-health-status {ok|info|warning|critical}]** - NFS Operational Status

Selects the items that match this parameter value.

**[-cifs-config-status {configured|notconfigured|disabled}]** - CIFS Configuration Status

Selects the items that match this parameter value.

**[-cifs-health-status {ok|info|warning|critical}]** - CIFS Operational Status

Selects the items that match this parameter value.

**[-lif-total <integer>]** - Number of LIFs

Selects the items that match this parameter value.

**[-lif-online <integer>]** - LIFs Online

Selects the items that match this parameter value.

**[-lif-offline <integer>]** - LIFs Offline

Selects the items that match this parameter value.

**[-lif-nothome <integer>]** - LIFs not home

Selects the items that match this parameter value.

**[-lif-no-failover <integer>]** - LIFs without Failover Rules

Selects the items that match this parameter value.

**[-lif-nohosted <integer>]** - Number of LIFS not hosted

Selects the items that match this parameter value.

**[-lif-home-port-down <integer>]** - LIFs With Home Port Down

Selects the items that match this parameter value.

**[-vol-total <integer>]** - Number of Volumes

Selects the items that match this parameter value.

**[-vol-online <integer>]** - Online Volumes

Selects the items that match this parameter value.

**[-vol-offline <integer>]** - Offline Volumes

Selects the items that match this parameter value.



---

**[-vol-full <integer>]** - Volumes Currently Full

Selects the items that match this parameter value.

**[-vol-restricted <integer>]** - Volumes Restricted

Selects the items that match this parameter value.

**[-root-vol-status {online|offline}]** - Root Volume State

Selects the items that match this parameter value.

**[-root-vol-state {ok|info|warning|critical}]** - Root Volume Health

Selects the items that match this parameter value.

**[-root-vol-mirrors-total <integer>]** - Root LS Mirrors

Selects the items that match this parameter value.

**[-root-vol-mirrors-online <integer>]** - Root LS Mirrors Online

Selects the items that match this parameter value.

**[-aggr-total <integer>]** - Aggregates

Selects the items that match this parameter value.

**[-aggr-online <integer>]** - Aggregates Online

Selects the items that match this parameter value.

**[-aggr-offline <integer>]** - Aggregates Offline

Selects the items that match this parameter value.

**[-aggr-failedover <integer>]** - Aggregates Failed-Over

Selects the items that match this parameter value. "Failed over" aggregates have failed over to a partner node.

**[-aggr-full <integer>]** - Aggregates That Are Full

Selects the items that match this parameter value. "Full" aggregates have exceeded their configured threshold.

**[-ports-total <integer>]** - Network Ports

Selects the items that match this parameter value.

**[-ports-shared <integer>]** - Network Ports Sharing Resources with Migrated LIFs

Selects the items that match this parameter value. "Shared" ports contain active logical interfaces that have failed over to a partner node.

**[-issues <text>, ...] - Health Issues**

Selects the items that match this parameter value.

**Examples**

The following example shows default Vserver health information:

```
cluster1::> dashboard health vsriver show
Vserver      Status  Health  EMS  Issues
-----
node1        online  warning  0    0    0
Issues: The Vserver root volume is online however there
are no mirrors of the root volume.
node2        online  warning  0    0    0
node3        online  warning  0    0    0
```

The following example shows detailed Vserver health information:

```
cluster1::> dashboard health vsriver show -vsriver node1 -instance
Vserver
-----
node1      Status: online      EMS Critical: 0
           Health: warning      Warning: 0
           Informational: 0

Issues: The Vserver root volume is online however there
are no load-sharing mirrors online.

Protocols
  NFS      Status: configured      Health: ok
  CIFS     Status: configured      Health: ok

LIFs
  Total: 4      Online: 4
                Offline: 0
                LIFs Not Home: 0
                LIFs Without Failover Rules: 4
                LIFs Not Hosted: 0
                LIFs With Home Port Down: 0

Volumes
  Total: 11     Online: 11
                Offline: 0
                Restricted: 0
                Full: 0

Root Volume
                State: online
                Health: warning
                Mirrors: 0
                Mirrors Online: 0

Resources
  Aggregates
    Total: 1     Online: 1
                Offline: 0
                Failed Over To Partner: 0
                Full: 0

Network Ports
  Total: 4      Ports With LIFs Not Home: 0
```

---

## dashboard performance show

Display per-second performance figures

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

### Description

The `dashboard performance show` command displays information about the performance of individual nodes and the cluster as a whole.

### Parameters

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

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

| **[-operations ]**

Displays the following information:

- Node name or cluster summary
- Average latency
- Total operations per second
- NFS latency
- NFS operations per second
- CIFS latency
- CIFS operations per second
- SPIN latency
- SPIN operations per second

| **[-instance ] }**

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

**[-node {<nodename>|local}]** - Node

---

Selects the items that match this parameter value.

**[-avg-latency <Counter64>]** - Average Latency (usec)

Selects the items that match this parameter value.

**[-cpu-busy <Counter>]** - CPU Busy

Selects the items that match this parameter value (percentage of CPU utilization).

**[-total-ops <Counter64>]** - Total Ops/s

Selects the items that match this parameter value.

**[-nfs-ops <Counter64>]** - NFS Ops/s

Selects the items that match this parameter value.

**[-cifs-ops <Counter64>]** - CIFS Ops/s

Selects the items that match this parameter value.

**[-data-busy <Counter>]** - Data Network Utilization

Selects the items that match this parameter value (percentage of data network utilization).

**[-data-recv <Counter64>]** - Data Network Received (per sec)

Selects the items that match this parameter value.

**[-data-sent <Counter64>]** - Data Network Sent (per sec)

Selects the items that match this parameter value (MB per second sent to the data network).

**[-cluster-busy <Counter>]** - Cluster Network Utilization

Selects the items that match this parameter value (percentage of cluster network utilization).

**[-cluster-recv <Counter64>]** - Cluster Network Received (per sec)

Selects the items that match this parameter value (MB per second received from the cluster network).

**[-cluster-sent <Counter64>]** - Cluster Network Sent (per sec)

Selects the items that match this parameter value (MB per second sent to the cluster network).

**[-storage-read <Counter64>]** - Storage Read (per sec)

Selects the items that match this parameter value (MB per second read from storage).

---

**[-storage-write <Counter64>]** - Storage Write (per sec)

Selects the items that match this parameter value (MB per second written to storage).

**[-cifs-latency <Counter64>]** - CIFS Average Latency

Selects the items that match this parameter value (in microseconds).

**[-nfs-latency <Counter64>]** - NFS Average Latency

Selects the items that match this parameter value (in microseconds).

## Examples

The following example shows standard performance dashboard information for a cluster:

```
cluster1::> dashboard performance show
      Total Average   ---Data-Network--- -Cluster--Network-  ---Storage---
      Ops/s Latency CPU Busy Recv Sent Busy Recv Sent Read Write
      ----- in usec Busy Util MB/s MB/s Util MB/s MB/s MB/s MB/s
node1      0      0    2%  0%      0      0  0%      0      0      0      0
node2      0      0    2%  0%      0      0  0%      0      0      0      0
cluster:summary
0      0    2%  0%      0      0  0%      0      0      0      0
3 entries were displayed.
```

The following example shows detailed performance-dashboard information for the node named node2:

```
cluster1::> dashboard performance show -node node2
Node: node2
Average Latency (usec): 624us
CPU Busy: 84%
Total Ops/s: 27275
NFS Ops/s: 27275
CIFS Ops/s: 0
Data Network Utilization: 0%
Data Network Received (MB/s): 0
Data Network Sent (MB/s): 0
Cluster Network Utilization: 0%
Cluster Network Received (MB/s): 0
Cluster Network Sent (MB/s): 0
Storage Read (MB/s): 0
Storage Write (MB/s): 0
CIFS Average Latency: 0us
NFS Average Latency: 624us
```

---

## dashboard storage show

Display storage dashboard

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

### Description

The `dashboard storage show` command displays information about storage utilization.

### Parameters

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

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

| [-performance ]

Displays storage space utilization and the current performance of I/O operations, including:

- Aggregate name
- Size
- Used space
- Percentage of space used
- Number of volumes
- Data read rate
- Number of I/O read operations per second
- Data write rate
- Number of I/O write operations per second
- Node names

| [-week ]

Displays the storage space utilization trend over the past seven days, including:

- 
- Aggregate name
  - Size
  - Used space
  - Number of volumes
  - One-day change in used size
  - One-day change in number of volumes
  - Two-day change in used size
  - Two-day change in number of volumes
  - Three-day change in used size
  - Three-day change in number of volumes
  - Seven-day change in used size
  - Seven-day change in number of volumes

| [-instance ] }

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

**[-aggregate <aggregate name>]** - Aggregate

Selects the aggregates that match this parameter value.

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

Selects the aggregates that match this parameter value.

**[-usedsize {<integer>[KB|MB|GB|TB|PB]}]** - Used Size

Selects the aggregates that match this parameter value.

**[-availsize {<integer>[KB|MB|GB|TB|PB]}]** - Avail Size

Selects the aggregates that match this parameter value.

**[-percent-used <percent>]** - Used%

Selects the aggregates that match this parameter value.

**[-nodes {<nodename>|local}, ...]** - Nodes

Selects the aggregates that match this parameter value.

**[-volcount <integer>]** - Volumes

---

Selects the aggregates that match this parameter value (number of volumes).

**[-read-data <Counter64>]** - Read Data MB/s

Selects the aggregates that match this parameter value.

**[-read-iops <Counter64>]** - Read IOPs

Selects the aggregates that match this parameter value.

**[-write-data <Counter64>]** - Write Data MB/s

Selects the aggregates that match this parameter value (MB per second written to storage).

**[-write-iops <Counter64>]** - Write IOPs

Selects the aggregates that match this parameter value.

**[-status <text>, ...]** - Status

Selects the aggregates that match this parameter value. Possible values are:

- creating
- failed
- offline
- online
- partial
- restricted
- unknown
- normal
- verifying
- snapmirrored
- copying
- ironing
- mirrored
- resyncing
- mirror degraded
- invalid
- needs check



- 
- initialized
  - growing
  - partial
  - degraded
  - noparity
  - reconstruct
  - out-of-date
  - foreign

Separate multiple values with commas.

**[-4h-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 4-hour Change in Used Size

Selects the aggregates that match this parameter value.

**[-4h-change-vols <integer>]** - 4-hour Change in Number of Volumes

Selects the aggregates that match this parameter value.

**[-8h-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 8-hour Change in Used Size

Selects the aggregates that match this parameter value.

**[-8h-change-vols <integer>]** - 8-hour Change in Number of Volumes

Selects the aggregates that match this parameter value.

**[-1d-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 1-day Change in Used Size

Selects the aggregates that match this parameter value.

**[-1d-change-vols <integer>]** - 1-day Change in Number of Volumes

Selects the aggregates that match this parameter value.

**[-2d-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 2-day Change in Used Size

Selects the aggregates that match this parameter value.

**[-2d-change-vols <integer>]** - 2-day Change in Number of Volumes

Selects the aggregates that match this parameter value.

**[-3d-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 3-day Change in Used Size

Selects the aggregates that match this parameter value.

**[-3d-change-vols <integer>]** - 3-day Change in Number of Volumes

---

Selects the aggregates that match this parameter value.

**[-7d-change-used {<integer>[KB|MB|GB|TB|PB]}]** - 7-day Change in Used Size

Selects the aggregates that match this parameter value.

**[-7d-change-vols <integer>]** - 7-day Change in Number of Volumes

Selects the aggregates that match this parameter value.

## Examples

The following example shows storage utilization information about the aggregate named `aggr1`:

```
cluster1::> dashboard storage show -aggregate aggr1

Aggregate: aggr1
Size: 6.21TB
Used Size: 5.14TB
Avail Size: 1.06TB
Used%: 83%
Nodes: node1
Volumes: 49
Read Data MB/s: 5904283
Read IOPs: 0
Write Data MB/s: 0
Write IOPs: 0
Status: online
4-hour Change in Used Size: 2.75GB
4-hour Change in #Volumes: 0
8-hour Change in Used Size: 15.81GB
8-hour Change in #Volumes: 0
1-day Change in Used Size: 16.50GB
1-day Change in #Volumes: 0
2-day Change in Used Size: 16.97GB
2-day Change in #Volumes: 0
3-day Change in Used Size: 62.62GB
3-day Change in #Volumes: 0
7-day Change in Used Size: 325.1GB
7-day Change in #Volumes: 0
```

---

## event config modify

Modify log configuration parameters

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

### Description

Use the `event config modify` command to configure event notification and logging for the cluster.

### Parameters

**[-mailfrom <mail address>]** - Mail From

Use this parameter to configure the e-mail address from which e-mail notifications will be sent. You can configure the cluster to send e-mail notifications when specific events occur. Use the `event route add-destinations` and `event destination create` commands to configure e-mail destinations for events.

**[-mailserver <Remote IP>]** - Mail Server (SMTP)

Use this parameter to configure the name or IP address of the SMTP server used by the cluster when sending e-mail notification of events.

**[-suppression {on|off}]** - Event Throttling/Suppression (privilege: advanced)

Use this parameter to configure whether event suppression algorithms are enabled ("on") or disabled ("off"). The event processing system implements several algorithms to throttle events. The documentation for `event show-suppression` describes the suppression algorithms in detail.

Note:

The suppression parameter can disable both autosuppression and duplicate suppression, but timer suppression cannot be disabled.

**[-console {on|off}]** - Console Logging (privilege: advanced)

Use this parameter to configure whether events are displayed on the console port ("on") or not ("off").

### Examples

---

The following command sets the "Mail From" address for event notifications to "admin@example.com" and the "Mail Server" to "mail.example.com".

```
cluster1::> event config modify -mailfrom admin@example.com -mailserver  
mail.example.com
```

The following example turns on event suppression and console logging.

```
cluster1::> event config modify -suppression on -console on
```

## See Also

event route add-destinations event destination create event show-suppression  
event log show event tracelog log show

---

## event config show

Display log configuration parameters

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

### Description

The `event config show` command displays information about the configuration of event notification and event logging for the cluster.

"Mail From" is the e-mail address that the event notification system uses as the "From" address for e-mail notifications.

"Mail Server" is the name or IP address of the SMTP server that the event notification system uses to send e-mail notification of events.

"Event Throttling/Suppression" indicates whether event suppression algorithms are enabled ("on") or disabled ("off"). The event processing system implements several algorithms to throttle events. See `event show-suppression` for suppression algorithm details.

Note:

The suppression parameter can disable both autosuppression and duplicate suppression, but not timer suppression.

"Console Logging" indicates whether events are displayed on the console port ("on") or not ("off").

### Parameters

None

### Examples

The following example displays the configuration of event notification for the cluster:

```
cluster1::> event config show
Mail From: admin@example.com
Mail Server: mail.example.com
```

### See Also

`event show-suppression` `event log show` `event tracelog log show`

---

## event destination create

Create an event destination

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

### Description

The `event destination create` command creates a new event destination. An event destination is a list of addresses that receive event notifications. These addresses can be e-mail addresses, SNMP trap hosts, and syslog servers. Event destinations are used by event routes. Event routes describe which events generate notifications, and event destinations describe where to send those notifications.

When you create a destination, you can add e-mail addresses, SNMP trap hosts, and syslog hosts to the definition of the destination. Once the destination is fully defined, use the `event route add-destinations` command to associate the destination with event routes so that notifications of those events are sent to the recipients in the destination.

To see the current list of all destinations and their recipients, use the `event destination show` command.

There are several default destinations provided for your use.

- `allevents` - A useful destination for all system events, though no events are routed to this destination by default.
- `asup` - Events routed to this destination trigger AutoSupport(tm). Only use this destination to send notifications to technical support. See `system node autosupport` for more information.
- `criticals` - A useful destination for critical events though no events are routed to this destination by default.
- `pager` - A useful destination for all events that are urgent enough to page a system administrator, though no events are routed to this destination by default.
- `traphost` - The default destination for all SNMP traps. You can also use the `system snmp traphost add` command to add SNMP recipients to the traphost default destination.

To add recipients to the default destinations, use the `event destination modify` command.

---

You should not create a destination that sends events to more than one type of recipient. Use separate destinations for e-mail, SNMP, and syslog activity. Also, use the traphost default destination for all SNMP activity. You must not create any other destination that sends traps to SNMP trap hosts. The traphost default destination is not required to be added to any event route.

## Parameters

**-name** <text> - Name

This mandatory parameter specifies name of the event destination to create.

**[-mail** <mail address>, ...] - Mail Destination

Use this parameter to specify one or more e-mail addresses to which event notifications will be sent. For events to properly generate e-mail notifications, the event system must also be configured with an address and mail server from which to send mail. See `event config modify` for more information.

**[-snmp** <Remote IP>, ...] - SNMP Destination

To send traps to SNMP trap hosts, use this parameter with the host names or IP addresses of those trap hosts.

**[-syslog** <Remote IP>, ...] - Syslog Destination

Use this parameter with the host names or IP addresses of any remote syslog daemons to which syslog entries will be sent.

**[-syslog-facility** <Syslog Facility>] - Syslog Facility

This parameter optionally specifies a syslog facility with which the syslog is sent. Possible values for this parameter are default, local0, local1, local2, local3, local4, local5, local6, and local7. If you specify the default syslog facility, syslogs are tagged LOG\_KERN or LOG\_USER.

**[-snmp-community** <text>] - SNMP Trap Community

To specify an SNMP trap community, use this parameter with that string.

**[-hide-parameters** {true|false}] - Hide Parameter Values?

Use this parameter with the value "true" to hide event parameters by removing them from event notifications. This is useful to prevent sensitive information from being sent over non-secure channels.

## Examples

---

The following example creates an event destination named support.email that e-mails events to the addresses supportmgr@example.com, techsupport@example.com, and oncall@example.com.

```
cluster1::> event destination create -name support.email -mail
supportmgr@example.com,techsupport@example.com,oncall@example.com
```

This example creates an event destination named support.bucket01 that sends the notifications to a syslog host.

```
cluster1::> event destination create -name support.bucket01 -syslog
loghost.example.com
```

## See Also

event config modify   event route add-destinations   event destination show  
system node autosupport   system snmp traphost add   event destination modify



---

## event destination delete

Delete an event destination

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

### Description

The `event destination delete` command removes a specified destination from the list of valid destinations. An event destination is a list of addresses that receive event notifications. These addresses can be e-mail addresses, SNMP trap hosts, and syslog servers. Event destinations are used by event routes. Event routes describe which events generate notifications, and event destinations describe where to send those notifications.

Once you delete a destination, you will not be able to add that destination to any event route.

You will not be able to delete a destination if it is in use by any event routes. To remove a destination from all event routes, so that you can delete it, use the `event route remove-destinations -messagename * -destination name` command.

There are several default destinations that cannot be deleted:

- `allevents` - A useful destination for all system events, though no events are routed to this destination by default.
- `asup` - Events routed to this destination trigger AutoSupport(tm). Only use this destination to send notifications to technical support. See `system node autosupport` for more information.
- `criticals` - A useful destination for critical events though no events are routed to this destination by default.
- `pager` - A useful destination for all events that are urgent enough to page a system administrator, though no events are routed to this destination by default.
- `traphost` - The default destination for all SNMP traps. You can also use the `system snmp traphost delete` command to delete SNMP recipients from the traphost default destination.

To see the current list of all destinations, use the `event destination show` command. To add a new destination to the list, use the `event destination create` command.

---

## Parameters

**-name** <text> - Name

This mandatory parameter specifies the event destination to delete.

## Examples

The following example deletes an event destination named manager.pager:

```
cluster1::> event destination delete -name manager.pager
```

## See Also

event route remove-destinations   system node autosupport  
system snmp traphost delete   event destination show   event destination create

---

## event destination modify

Modify an event destination

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

### Description

The `event destination modify` command changes the definition of an existing event destination. An event destination is a list of addresses that receive event notifications. These addresses can be e-mail addresses, SNMP traphosts, and syslog servers. Event destinations are used by event routes. Event routes describe which events generate notifications, and event destinations describe where to send those notifications.

Modifying a parameter writes over the existing value of the parameter. To extend a parameter, make sure to include the current value of that parameter. For instance, to add an e-mail address to a destination, include all of the current e-mail addresses assigned to that destination along with the new address. To see the current definition of a destination, use the `event destination show -name name` command.

You must not create a destination that sends events to more than one type of recipient. Use separate destinations for e-mail, SNMP, and syslog activity. Also, use the traphost default destination for all SNMP activity. You should not create any other destination that sends to SNMP traphosts. The traphost default destination is not required to be added to any event route.

### Parameters

**-name <text>** - Name

This mandatory parameter specifies name of the event destination to modify.

**[-mail <mail address>, ...]** - Mail Destination

Use this parameter to specify one or more e-mail addresses to which event notifications will be sent. For events to properly generate e-mail notifications, the event system must also be configured with an address and mail server from which to send mail. See `event config modify` for more information.

**[-snmp <Remote IP>, ...]** - SNMP Destination

To send traps to SNMP trap hosts, use this parameter with the host names or IP addresses of those trap hosts.

---

### **[-syslog <Remote IP>, ...] - Syslog Destination**

Use this parameter with the host names or IP addresses of any remote syslog daemons to which syslog entries will be sent.

### **[-syslog-facility <Syslog Facility>] - Syslog Facility**

This parameter optionally specifies a syslog facility with which the syslog is sent. Possible values for this parameter are default, local0, local1, local2, local3, local4, local5, local6, and local7. If you specify the default syslog facility, syslogs are tagged LOG\_KERN or LOG\_USER.

### **[-snmp-community <text>] - SNMP Trap Community**

To specify an SNMP trap community, use this parameter with that string.

### **[-hide-parameters {true|false}] - Hide Parameter Values?**

Enter this parameter with the value "true" to hide event parameters by removing them from event notifications. This is useful to prevent sensitive information from being sent over non-secure channels. Enter it with the value "false" to turn off parameter hiding.

## **Examples**

The following example modifies an event destination named snmp.hosts to send events to SNMP trap hosts named traphost1 and traphost2:

```
cluster1::> event destination modify -name snmp.hosts -snmp
traphost1.example.com,traphost2.example.com
```

This example adds the e-mail address of a remote support facility to an existing list of e-mail recipients.

```
cluster1::> event destination show -name support
      Name: support
      Mail Destination: support.hq@company.com
      SNMP Destination: -
      Syslog Destination: -
      Syslog Facility: -
      SNMP Trap Community: -
      Hide Parameter Values?: -

cluster1::> event destination modify -name support -mail
support.hq@company.com,support.remote@company.com

cluster1::> event destination show -name support
      Name: support
      Mail Destination: support.hq@company.com, support.remote@company.com
      SNMP Destination: -
      Syslog Destination: -
      Syslog Facility: -
      SNMP Trap Community: -
      Hide Parameter Values?: -
```

## **See Also**

---

event config modify   event destination show

---

## event destination show

Display event destinations

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

### Description

The `event destination show` command displays information about configured event destinations. An event destination is a list of addresses that receive event notifications. These addresses can be e-mail addresses, SNMP trap hosts, and syslog servers. Event destinations are used by event routes. Event routes describe which events generate notifications, and event destinations describe where to send those notifications.

Default destinations:

- `allevents` - A useful destination for all system events, though no events are routed to this destination by default.
- `asup` - Events routed to this destination trigger AutoSupport(tm). Only use this destination to send notifications to technical support. See `system node autosupport` for more information.
- `criticals` - A useful destination for critical events although no events are routed to this destination by default.
- `pager` - A useful destination for all events that are urgent enough to page a system administrator, though no events are routed to this destination by default.
- `traphost` - The default destination for all SNMP traps. You can also use the `system snmp traphost show` command to view SNMP recipients for the traphost default destination.

To add recipients to the default destination, use the `event destination modify` command.

Note:

While you can use both host names and IP addresses with parameters, only IP addresses are stored. Unless all DNS and reverse-DNS operations complete successfully, IP addresses might appear in command output.

---

## Parameters

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

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

| **[-facility ]**

Displays only the syslog destinations and syslog facilities.

| **[-instance ] }**

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

**[-name <text>]** - Name

Selects the destinations that match this parameter value.

**[-mail <mail address>, ...]** - Mail Destination

Selects the destinations that match this parameter value.

**[-snmp <Remote IP>, ...]** - SNMP Destination

Selects the destinations that match this parameter value (SNMP trap hosts).

**[-syslog <Remote IP>, ...]** - Syslog Destination

Selects the destinations that match this parameter value (syslog event notification daemons).

**[-syslog-facility <Syslog Facility>]** - Syslog Facility

Selects the destinations that match this parameter value. Valid values are: `default`, `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, and `local7`.

**[-snmp-community <text>]** - SNMP Trap Community

Selects the destinations that match this parameter value.

**[-hide-parameters {true|false}]** - Hide Parameter Values?

Selects the destinations that match this parameter value (`true` selects destinations that do not receive full event parameters, `false` selects destinations that receive full event parameters). Event parameters may be hidden to prevent sensitive information from being sent over non-secure channels.

## Examples

The following example displays information about all event destinations:

```
cluster1::> event destination show
```

Name	Mail Dest.	SNMP Dest.	Syslog Dest.	Hide Params
allevents	-	-	logger.example.com	-
asup	-	-	-	-
criticals	oncall @example.com	-	-	-
pager	pager@example.com	-	-	-
support.email	supportmgr @example.com, techsupport @example.com, oncall @example.com	-	-	-
traphost	-	th0.example.com, th1.example.com	-	-

6 entries were displayed.

**See Also**

system node autosupport   system snmp traphost show   event destination modify



---

## event log show

Display latest log events

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

### Description

The `event log show` command displays the contents of the event log, which lists significant occurrences within the cluster. Events are categorized by type. Use the `event route show` command to display general information about each type of event.

By default, the command displays non-DEBUG severity level events with the following information, with the most recent events listed first:

- The node on which the event occurred
- The sequence number of the event
- The time at which the event occurred
- The severity of the event
- The source of the event
- The event's message name

To display detailed information about events, use one or more of the optional parameters that affect how the command output is displayed and the amount of detail that is included. For example, to display all detailed event information, use the `-detail` parameter.

To display DEBUG severity level events, use the `-severity` parameter.

At the advanced privilege level and higher, the command displays the following additional information:

- The internal EMS severity of the event
- The event's kernel generation number, if applicable
- The event's kernel sequence number, if applicable

---

This command only shows information about the occurrence of an event. To see information about the significance of an event, use the `event route show` command. It describes the event in more detail, and suggests possible corrective actions.

## Parameters

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

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

| **[-detail ]**

Displays all detailed event information.

| **[-detailtime ]**

Displays detailed event information in chronological order.

| **[-instance ] }**

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

**[-node {<nodename>|local}]** - Node

Displays a list of events for the node you specify. Use this parameter with the `-seqnum` parameter to display detailed information.

**[-seqnum <Sequence Number>]** - Sequence#

Selects the events that match this parameter value. Use with the `-node` parameter to display detailed information.

**[-time <MM/DD/YYYY HH:MM:SS>]** - Time

Selects the events that match this parameter value. Use the format: MM/DD/YYYY HH:MM:SS [+ HH:MM]. You can specify a time range by using the `".."` operator between two time statements.

```
show -time "08/13/2010 05:55:00".. "08/13/2010 06:10:00"
```

Comparative time values are relative to "now". For example, to display only events that occurred within the last minute:

```
show -time >1m
```

**[-severity {EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFORMATIONAL|DEBUG}]** - Severity

Selects the events that match this parameter value. Severity levels:

- 
- EMERGENCY - The system is unusable
  - ALERT - Action must be taken immediately
  - CRITICAL - Critical condition
  - ERROR - Error condition
  - WARNING - Warning condition
  - NOTICE - Normal but significant condition
  - INFORMATIONAL - Information message
  - DEBUG - Debugging message

To display all events, including ones with a severity of DEBUG, specify severity as follows:

```
show -severity <=DEBUG
```

**[-ems-severity {NODE\_FAULT|SVC\_FAULT|NODE\_ERROR|SVC\_ERROR|WARNING|NOTICE|INFO|DEBUG|VAR}]** - EMS Severity (privilege: advanced)

Selects the events that match this parameter value. Severity levels:

- NODE\_FAULT - Data corruption has been detected or the node is unable to provide client service
- SVC\_FAULT - A temporary loss of service, typically a transient software fault, has been detected
- NODE\_ERROR - A hardware error that is not immediately fatal has been detected
- SVC\_ERROR - A software error that is not immediately fatal has been detected
- WARNING - A high-priority message that does not indicate a fault
- NOTICE - A normal-priority message that does not indicate a fault
- INFO - A low-priority message that does not indicate a fault
- DEBUG - A debugging message
- VAR - A message with variable severity, selected at runtime.

**[-source <text>]** - Source

Selects the events that match this parameter value (typically a software module).

**[-messagename <Message Name>]** - Message Name

Selects the events that match this parameter value (string). Message names are descriptive, so filtering output by message name displays messages of a specific type.

---

### **[-event <text>] - Event**

Selects the events that match this parameter value. This parameter is most useful when entered with wildcards. The "event" field contains the full text of the event, including any parameters. For example, a waf1.vol.offline event will contain the name of the volume taken offline.

### **[-kernelgen <integer>] - Kernel Generation Number (privilege: advanced)**

Selects the events that match this parameter value. Only events that emanate from the kernel have kernel generation numbers.

### **[-kernelseqnum <integer>] - Kernel Sequence Number (privilege: advanced)**

Selects the events that match this parameter value. Only events that emanate from the kernel have kernel sequence numbers.

## **Examples**

The following example displays the event log:

```
cluster1::> event log show
Time           Node           Severity           Event
-----
11/9/2010 13:54:19 node1      INFORMATIONAL      vifmgr.portup: A link up event
was received on node node1, port e0a.
11/9/2010 13:54:19 node1      INFORMATIONAL      vifmgr.portup: A link up event
was received on node node1, port e0d.
11/9/2010 13:54:19 node1      INFORMATIONAL      vifmgr.portup: A link up event
was received on node node1, port e0c.
11/9/2010 13:54:19 node1      INFORMATIONAL      vifmgr.portup: A link up event
was received on node node1, port e0b.
...
```

This example demonstrates how to use a range with the `-time` parameter to display all events that occurred during an extended time period. It displays all events that occurred between 1:45pm and 1:50pm on November 9, 2010.

```
cluster1::> event log show -time "11/9/2010 13:45:00".. "11/9/2010 13:50:0"
```

The `-time` parameter also accepts values that are relative to "now". The following example displays events that occurred more than one hour ago.

```
cluster1::event log> show -time <1h
Time           Node           Severity           Event
-----
11/9/2010 13:02:03 node1      NOTICE           raid.spares.media_scrub.start:
owner="", disk_info="Disk v5.32 Shelf ? Bay ? [
[14463913]", blockNum="5248", shelf="?", bay="?", vendor=" ", model="VD-1000MB-
FZ-520", firmware_revision="0042", serialno="14463913", disk_type="2",
disk_rpm="15000"
11/9/2010 13:02:03 node1      NOTICE           raid.spares.media_scrub.start:
owner="", disk_info="Disk v5.29 Shelf ? Bay ? [
[14463912]", blockNum="5248", shelf="?", bay="?", vendor=" ", model="VD-1000MB-
FZ-520", firmware_revision="0042", serialno="14463912", disk_type="2",
disk_rpm="15000"
...
```

---

Severity levels sort in the order opposite to what you might expect. The following example displays all events that have a severity level of CRITICAL or more severe.

```
cluster1::> event log show -severity <CRITICAL
```

## **See Also**

event route show

---

## event mailhistory delete

Delete an e-mail history record

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

### Description

The `event mailhistory delete` command deletes a record from the e-mail history.

To delete a record, you must know which node contains the record, and the record's sequence number. Use the `event mailhistory show` command to view this information.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node that contains the e-mail history record to delete.

**-seqnum** <Sequence Number> - Sequence Number

Use this parameter to specify the sequence number of the e-mail history record to delete.

### Examples

The following example deletes all mail-history records on node1:

```
cluster1::> event mailhistory delete -node node1 -seqnum *
```

### See Also

`event mailhistory show`

---

## event mailhistory show

Display a list of e-mail history records

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

### Description

The `event mailhistory show` command displays a list of the event notifications that have been e-mailed. The command output depends on the parameters you specify with the command. By default, the command displays basic information about all notification e-mails that were sent.

To display detailed information about a specific mail-history record, run the command with the `-seqnum` parameter.

### Parameters

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

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

| **[-instance** ] }

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

**[-node** {<nodename>|local}] - Node

Selects the mail-history records that match this parameter value.

**[-seqnum** <Sequence Number>] - Sequence Number

Selects the mail-history records that match this parameter value.

**[-messagename** <Message Name>] - Message Name

Selects the mail-history records that match this parameter value.

**[-address** <mail address>, ...] - Mail Address

Selects the mail-history records that match this parameter value.

**[-time** <MM/DD/YYYY HH:MM:SS>] - Transmission Time

---

Selects the mail-history records that match this parameter value.

**[-message <text>]** - Alert Message

Selects the mail-history records that match this parameter value (text pattern).

**[-previous-time <MM/DD/YYYY HH:MM:SS>]** - Previous Transmission Time

Selects the mail-history records that match this parameter value.

**[-num-drops-since-previous <integer>]** - Number of Drops Since Previous Transmission

Selects the mail-history records that match this parameter value (number of event drops since last transmission).

## Examples

The following example displays detailed information about the mail-history record with the sequence number 20520:

```
cluster1::> event mailhistory show -seqnum 20520
  Sequence Number: 20520
    Message Name:  waf1.vol.full
      Address:    admin@example.com
        Time:     10/1/2008 14:06:24
        Node:     node3
    Previous Time: 5/31/2007 00:33:22
# Drops Since Prev: 0
  Mail Message:   waf1.vol.full: file system on volume
                  vol10@vserver:28558fe3-2462-11da-85ab
                  -000423bacd20 is full
```



---

## event route add-destinations

Add destination(s) to an event definition

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

### Description

The `event route add-destinations` command adds destinations to an event route. Any existing destinations assigned to the route are not removed.

The destinations you add must already exist. See the documentation for the `event destination create` command for information about creating destinations. To show all existing destinations and their attributes, use the `event destination show` command. To remove destinations from an event route, use the `event route remove-destinations` command.

You can use extended queries with such parameters as `-severity` and `-snmp-support` to specify multiple events that meet certain criteria. See examples below that show how to use extended queries.

### Parameters

**-messagename** <Message Name> - Message Name

Specify the message name of the event you are modifying. You can use wildcards to specify a family of events or type of event.

**-destinations** <Event Destination>, ... - Destinations

Use this optional parameter to specify a comma-separated list of destinations to which notifications for the named event are sent. These destinations will be added to any existing destinations assigned to this event route.

### Examples

The following example specifies that all RAID events go to the destinations named `support.email`, `mgr.email`, and `sreng.pager`:

```
cluster1::> event route add-destinations -messagename raid* -destinations
support.email,mgr.email,sreng.pager
```

The following example specifies that all critical, alert, and emergency events go to the destination named `test_dest`:

```
cluster1::> event route add-destinations {-severity <=CRITICAL} -destinations
test_dest
```

---

The following example specifies that all critical or alert events that support a SNMP trap go to the destination named traphost:

```
cluster1::> event route add-destinations {-snmp-support true -severity CRITICAL|  
ALERT} -destinations traphost
```

## See Also

event destination create   event destination show   event route remove-destinations

---

## event route modify

Modify an event's destination, reporting threshold, or both

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

### Description

Use the `event route modify` command to modify an event's destination, frequency threshold, and time threshold. The event's destination must already exist; see the documentation for the `event destination create` command for information about creating destinations. The frequency threshold and time threshold prevent multiple event notifications in a brief period of time.

You can use extended queries with such parameters as `-severity` and `-snmp-support` to specify multiple events that meet certain criteria. See examples provided in the `event route add-destinations` command manpage that show how to use extended queries.

The frequency threshold specifies the number of times an event occurs before a repeat notification of the event is sent; for instance, a frequency threshold of 5 indicates that a notification is sent every fifth time an event occurs. The time threshold specifies the number of seconds between notifications for an event; for instance, a time threshold of 120 indicates that a notification is sent only if it has been two minutes or more since the last notification for that event was sent.

If both the frequency threshold and time threshold are set, a notification is sent if either threshold is met. For instance, if the frequency threshold is set to 5 and the time threshold is set to 120, and the event occurs more than five times within two minutes, a notification is sent. If both thresholds are set to 0 (zero) or empty ("-"), there is no suppression of multiple event notifications.

### Parameters

**-messagename** <Message Name> - Message Name

Specify the message name of the event you are modifying. You can use wildcards to specify a family of events or type of event.

**[-destinations** <Event Destination>, ...] - Destinations

Use this optional parameter to specify a comma-separated list of destinations to which notifications for the named event are sent. Using this parameter replaces the current list of destinations with the list of destinations you specify. To add or remove individual

---

destinations from the current list, use `event route add-destinations` or `event route remove-destinations`.

**[-frequencythreshold <integer>]** - Number of Drops Between Transmissions

Specifies the number of event notifications that must occur within the `timethreshold` period before a repeat notification is sent.

**[-timethreshold <integer>]** - Dropping Interval (Seconds) Between Transmissions

If multiple notifications of an event occur within this many seconds, only the first notification is sent. Multiple notifications will be sent during this time period only if the `frequencythreshold` quantity is exceeded.

## Examples

The following example modifies all RAID events to send messages to a destination named "support.email", and specify that multiple messages should only be sent if and event occurs more than five times within 60 seconds.

```
cluster1::> event route modify -messagename raid* -destinations support.email -  
frequencythreshold 5 -timethreshold 60
```

## See Also

`event route add-destinations`   `event route remove-destinations`  
`event destination create`

---

## event route remove-destinations

Remove destination(s) from an event definition

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

### Description

The `event route remove-destinations` command can be used to remove existing destinations from an event route. This command removes only the specified destinations from the route, leaving any other destinations assigned to that route.

The named destinations are not deleted, just removed from the specified event route. To delete a destination entirely, use the `event destination delete` command. To show all existing destinations and their attributes, use the `event destination show` command.

You can use extended queries with such parameters as `-severity` and `-snmp-support` to specify multiple events that meet certain criteria. See examples provided in the `event route add-destinations` command manpage that show how to use extended queries.

### Parameters

**-messagename** <Message Name> - Message Name

Specify the message name of the event you are modifying. You can use wildcards to specify a family of events or type of event.

**-destinations** <Event Destination>, ... - Destinations

Use this optional parameter to specify a comma-separated list of destinations to remove from the event's list of destinations.

### Examples

The following example specifies that the destination named "mgr.email" should no longer receive notifications of RAID events.

```
cluster1::> event route remove-destinations -messagename raid* -destinations mgr.email
```

### See Also

`event destination delete`   `event destination show`   `event route add-destinations`

---

## event route show

Display event routes

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

### Description

This command displays information about event routes. Event routes describe which events generate notifications. A route specifies what to watch for, whom to notify, and what to do should a particular event occur. By default, the command displays the following information:

- Message name of the event
- Severity of the event
- Destinations for event notifications
- Frequency threshold for event notifications
- Time threshold for event notifications

To display detailed information about a specific event route, run the command with the `-messagename` parameter, and specify the name of the message. The detailed view adds the following information:

- Full description of the event
- Action to be taken to address the event

You can specify additional parameters to limit output to the information that matches those parameters. For example, to display information only about events with a message name that begins with "raid", run the command with the `-messagename raid*` parameter. You can enter either a specific text string or a wildcard pattern.

### Parameters

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

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

| [-instance ] }

---

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

**`[-messagename <Message Name>]`** - Message Name

Selects the event routes that match this parameter value.

**`[-severity {EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFORMATIONAL|DEBUG}]`** - Severity

Selects the event routes that match this parameter value. Valid values:

- EMERGENCY - The system is unusable
- ALERT - Action must be taken immediately
- CRITICAL - Critical condition
- ERROR - Error condition
- WARNING - Warning condition
- NOTICE - Normal but significant condition
- INFORMATIONAL - Information message
- DEBUG - Debugging message

**`[-action <text>]`** - Action

Selects the event routes that match this parameter value (text pattern).

**`[-description <text>]`** - Description

Selects the event routes that match this parameter value (text pattern).

**`[-snmp-support {true|false}]`** - Supports SNMP trap

Selects the event routes that match this parameter value.

**`[-destinations <Event Destination>, ...]`** - Destinations

Selects the event routes that match this parameter value. A destination is a list of email addresses, SNMP clients, and syslogs.

**`[-frequencythreshold <integer>]`** - Number of Drops Between Transmissions

Selects the event routes that match this parameter value (number of events since previous notification).

**`[-timethreshold <integer>]`** - Dropping Interval (Seconds) Between Transmissions

Selects the event routes that match this parameter value.

---

# Examples

The following example displays information about all event routes:

```
cluster1::> event route show
```

Message	Severity	Destinations	Freq Threshd	Time Threshd
admin.config.backup. push.fail	ERROR	allevents, pager	5	120
admin.config.changed	INFO	allevents	0	0
admin.config.url. unreachable	WARNING	allevents	0	0
admin.file.deleted	INFO	allevents	0	0
admin.login.failure	INFO	allevents	0	0
admin.software. commit.failure	ERROR	criticals, allevents	0	0
admin.software. commit.success	INFO	allevents	0	0
admin.software. committing	INFO	allevents	0	0
admin.software. installed	INFO	allevents	0	0
aggrcopy.dst. autoRestrictMsg	NOTICE	allevents	0	0
aggrcopy.dst. noMemory	ERROR	pager, admin	4	300
...				



---

## event snmphistory delete

Delete an SNMP trap history record

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

### Description

The `event snmphistory delete` command deletes an SNMP trap-history record. To delete a record, you will need to know which node generated the event, and you will need to know the sequence number of that event in the trap-history.

Use the `event snmphistory show` command to display a list of trap-history records and their sequence numbers.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node that contains the snmp history record to delete.

**-seqnum** <Sequence Number> - Sequence Number

Use this parameter to specify the sequence number of the SNMP trap-history record to delete.

### Examples

The following example deletes all SNMP trap-history records on node1:

```
cluster1::> event snmphistory delete -node node1 -seqnum *
```

### See Also

`event snmphistory show`

---

## event snmphistory show

Display a list of SNMP trap history records

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

### Description

The `event snmphistory show` command displays a list of event notifications that have been sent to SNMP traps. The command output depends on the parameters specified with the command. By default, the command displays general information about all trap-history records.

To display detailed information about a specific trap-history record, run the command with the `-seqnum` parameter.

### Parameters

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

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

| **[-instance** ] }

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

**[-node** {<nodename>|local}] - Node

Selects the trap-history records that match this parameter value (text pattern).

**[-seqnum** <Sequence Number>] - Sequence Number

Selects the trap-history records that match this parameter value (sequence number).

**[-messagename** <Message Name>] - Message Name

Selects the trap-history records that match this parameter value.

**[-address** <text>, ...] - SNMP Client Address

Selects the trap-history records that match this parameter value (IP address).

**[-time** <MM/DD/YYYY HH:MM:SS>] - Transmission Time

---

Selects the trap-history records that match this parameter value.

**[-message <text>]** - Alert Message

Selects the trap-history records that match this parameter value (text pattern).

**[-previous-time <MM/DD/YYYY HH:MM:SS>]** - Previous Transmission Time

Selects the trap-history records that match this parameter value.

**[-num-drops-since-previous <integer>]** - Number of Drops Since Previous Transmission

Selects the trap-history records that match this parameter value (number of event drops since last transmission).

## Examples

The following example displays information about all SNMP trap-history records:

```
cluster1::> event snmphistory show
Seq # Message Name      Address      Node  Time
-----
12481 raid.mirror.restrict 10.0.2.20 node0 4/14/2008 15:11:04
12482 aggrcopy.dst.noMemory 10.0.2.20 node0 4/14/2008 14:52:54
12483 raid.mirror.restrict 10.0.2.21 node1 4/14/2008 14:41:04
```

---

## event status show

Display event status

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

### Description

The `event status show` command summarizes information about occurrences of events. For detailed information about specific occurrences of events, use the `event log show` command.

### Parameters

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

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

| **[-instance** ] }

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

**[-node** {<nodename>|local}] - Node

Selects the event records that match this parameter value. Events are tracked on a node-by-node basis, rather than being rolled up cluster-wide.

**[-messagename** <Message Name>] - Message Name

Selects the event records that match this parameter value. The message name is a short descriptive string. Filtering output by message name displays messages of a specific type.

**[-indications** <integer>] - Number of Indications

Selects the event records that match this parameter value. This parameter is most useful when used with a range, such as using the range `">20"` to display only events that have been posted more than 20 times.

**[-drops** <integer>] - Number of Drops

Selects the event records that match this parameter value.

---

**[-last-time-occurred <MM/DD/YYYY HH:MM:SS>]** - Last Indication Time

Selects the event records that match this parameter value.

**[-last-time-dropped <MM/DD/YYYY HH:MM:SS>]** - Last Dropped Indication Time

Selects the event records that match this parameter value.

**[-last-time-processed <MM/DD/YYYY HH:MM:SS>]** - Last Processed Indication Time

Selects the event records that match this parameter value.

**[-stat-starting-time <MM/DD/YYYY HH:MM:SS>]** - Stat Starting Time

Selects the event records that match this parameter value.

**[-last-hour-histogram <integer>, ...]** - 60-minute Histogram (privilege: advanced)

Use this parameter with the `-fields` parameter to display the "last hour" histogram for each event type. The last hour histogram records the number of times each event occurred in the last hour. The histogram is divided into sixty buckets, and each bucket collects one minute's events. The buckets display with the most recent event first.

**[-last-day-histogram <integer>, ...]** - 24-hour Histogram (privilege: advanced)

Use this parameter with the `-fields` parameter to display the "last day" histogram for each event type. The last day histogram records the number of times each event occurred in the last day. The histogram is divided into 24 buckets, and each bucket collects one hour's events. The buckets display with the most recent event first.

**[-last-week-histogram <integer>, ...]** - 7-day Histogram (privilege: advanced)

Use this parameter with the `-fields` parameter to display the "last week" histogram for each event type. The last week histogram records the number of times each event occurred in the last week. The histogram is divided into 7 buckets, and each bucket collects one day's events. The buckets display with the most recent event first.

**[-severity {NODE\_FAULT|SVC\_FAULT|NODE\_ERROR|SVC\_ERROR|WARNING|NOTICE|INFO|DEBUG|VAR}]** - Severity

Selects events that have the event severity you specify. Severity levels sort with the most severe levels first. Severity levels:

- **NODE\_FAULT** - The node has detected data corruption, or is unable to provide client service.
- **SVC\_FAULT** - The node has detected a temporary loss of service. Typically, this is caused by a transient software fault.
- **NODE\_ERROR** - The node has detected a hardware error that is not immediately fatal.

- SVC\_ERROR - The node has detected a software error that is not immediately fatal.
- WARNING - A high-priority message that does not indicate a fault.
- NOTICE - A normal-priority message that does not indicate a fault.
- INFO - A low-priority message that does not indicate a fault.
- DEBUG - A debugging message. These messages are typically suppressed.
- VAR - These messages have variable severity. Severity level for these messages is selected at runtime.

The examples below illustrate how to query on severity.

## Examples

The following example displays recent event-occurrence status for node1:

```
cluster1::> event status show -node node1
Node      Message                                     Occurs Drops Last Time
-----
node1     raid.spares.media_scrub.start             6      0    3/11/2010 15:59:00
node1     raid.uninitialized.parity.vol             3      0    3/11/2010 15:58:28
node1     raid.vol.state.online                     3      0    3/11/2010 15:58:29
node1     reg.defaultCommit.set.timeTaken           1      0    3/11/2010 15:58:28
node1     scsitgt.ha.state.changed                  2      0    3/11/2010 15:58:28
node1     ses.multipath.notSupported                 2      0    3/11/2010 15:58:43
node1     shelf.config.mpha                         1      0    3/11/2010 15:58:48
node1     sk.hog.runtime                           1      0    3/11/2010 15:58:28
node1     snmp.agent.msg.access.denied              1      0    3/11/2010 15:58:28
node1     snmp.link.up                             6      0    3/11/2010 15:58:28
node1     tar.csum.mismatch                         2      0    3/11/2010 15:58:28
node1     tar.extract.success                       2      0    3/11/2010 15:58:28
node1     vifmgr.lifessuccessfullymoved             3      0    3/11/2010 15:58:46
node1     vifmgr.portdown                          1      0    3/11/2010 15:58:48
node1     vifmgr.portup                            5      0    3/11/2010 15:58:48
node1     vifmgr.startedsuccessfully                1      0    3/11/2010 15:58:43
```

The following example displays a summary of events which are warnings or more severe:

```
cluster1::> event status show -node node1 -severity <=warning -fields
indications,drops,severity
node  messagename             indications drops severity
-----
node1 api.output.invalidSchema    5463      840    WARNING
node1 callhome.dsk.config        1         0      WARNING
node1 callhome.sys.config      1         0      SVC_ERROR
node1 cecc_log.dropped          145       0      WARNING
node1 cecc_log.entry            5         0      WARNING
node1 cecc_log.entry_no_syslog  4540     218     WARNING
node1 cecc_log.summary          5         0      WARNING
node1 cf.fm.noPartnerVariable    5469     839     WARNING
node1 cf.fm.notkoverBadMbox      1         0      WARNING
node1 cf.fm.notkoverClusterDisable 1         0      WARNING
node1 cf.fsm.backupMailboxError  1         0      WARNING
node1 cf.takeover.disabled      23        0      WARNING
node1 cmds.sysconf.logErr       1         0      NODE_ERROR
node1 config.noPartnerDisks     1         0      NODE_ERROR
node1 fci.initialization.failed  2         0      NODE_ERROR
node1 fcp.service.adapter        1         0      WARNING
node1 fmmb.BlobNotFound          1         0      WARNING
node1 ha.takeoverImpNotDef       1         0      WARNING
```

---

```
node1    httpd.config.mime.missing 2      0    WARNING
node1    mgr.opsmgr.autoreg.norec 1      0    WARNING
node1    monitor.globalStatus.critical 1  0    NODE_ERROR
node1    raid.mirror.vote.versionZero 1  0    SVC_ERROR
node1    ses.multipath.notSupported 2     0    NODE_ERROR
node1    snmp.agent.msg.access.denied 1   0    WARNING
24 entries were displayed.
```

The above example makes use of several features which are common to all `show` commands:

- A query is specified for the severity parameter. A query restricts the output of the `show` command; only rows matching the query will be displayed. In this case, the query indicates that only events which have a severity of "WARNING" or more severe will be displayed.
- The fields parameter selects the fields to display. Note that the severity field is not displayed in the default output.

## See Also

`event show-suppression` `event config modify` `event log show`

---

## job delete

Delete a job

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

### Description

The `job delete` command deletes a job. Use the `job show` command to view a list of running jobs that can be deleted.

### Parameters

**-id** <integer> - Job ID

The numeric ID of the job you want to delete. A job ID is a positive integer.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example deletes the job that has ID 99:

```
cluster1::> job delete -id 99
```

### See Also

`job show`



---

## job pause

Pause a job

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

### Description

The `job pause` command pauses a job. Use the `job resume` command to resume a paused job. Use the `job show` command to view a list of running jobs that can be paused.

### Parameters

**-id** <integer> - Job ID

The numeric ID of the job you want to pause. A job ID is a positive integer.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example pauses the job that has ID 183:

```
cluster1::> job pause -id 183
```

### See Also

`job resume` `job show`

---

## job resume

Resume a job

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

### Description

The `job resume` command resumes a job that was previously paused by using the `job pause` command. Use the `job show` command to view a list of paused jobs that can be resumed.

### Parameters

**-id** <integer> - Job ID

The numeric ID of the paused job to be resumed. A job ID is a positive integer.

**-vserver** <vserver name> - Owning Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example resumes the paused job that has ID 183:

```
cluster1::> job resume -id 183
```

### See Also

`job pause` `job show`

---

## job show-bynode

Display a list of jobs by node

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

### Description

The `job show-bynode` command displays information about jobs on a per-node basis. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays information about all jobs in the cluster that are currently owned by a node.

To display detailed information about a specific job, run the command with the `-id` parameter. The detailed view includes all of the default information plus additional items.

You can specify additional parameters to display only information that matches the values you specify for those parameters. For example, to display information only about jobs running on a specific node, run the command with the `-node` parameter.

### Parameters

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

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

| **[-instance ]** }

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

**[-node {<nodename>|local}]** - Node

Use this parameter to display information only about the jobs that are associated with the node you specify.

**[-id <integer>]** - Job ID

Use this parameter to display information only about the jobs that match the ID or range of IDs you specify.

**[-vserver <vserver name>]** - Owning Vserver

---

Use this parameter with the name of a Vserver to display only jobs that are owned by that Vserver.

**[-name <text>]** - Name

Use this parameter to display information only about the jobs that match the job name you specify.

**[-description <text>]** - Description

Use this parameter to display information only about the jobs that match the description you specify.

**[-affinity {Cluster|Node}]** - Affinity

Use this parameter with an affinity value to display only jobs that match the affinity you specify.

**[-username <text>]** - User Name

Use this parameter with a username to display only jobs that are associated with that user.

## Examples

The following example displays information about all jobs on a per-node basis:

```
node::> job show-bynode
```

Node	Job ID	Name	Owning Vserver	Affinity
node0	1501	log-rotation	node-vserver	Cluster
	Descr:logrotation job			
node1	1498	log-rotation	node-vserver	Cluster
	Descr:logrotation job			
node2	1499	log-rotation	node-vserver	Cluster
	Descr:logrotation job			
node3	1500	log-rotation	node-vserver	Cluster
	Descr:logrotation job			

---

## job show-cluster

Display a list of cluster jobs

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

### Description

The `job show-cluster` command displays information about cluster-affiliated jobs. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays information about all cluster-affiliated jobs.

To display detailed information about a specific job, run the command with the `-id` parameter. The detailed view includes all of the default information plus additional items.

You can specify additional parameters to display only information that matches the values you specify for those parameters. For example, to display information only about jobs running on a specific node, run the command with the `-node` parameter.

### Parameters

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

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

| **[-instance ]** }

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

**[-id <integer>]** - Job ID

Use this parameter to display information only about the jobs that match the ID or range of IDs you specify.

**[-vserver <vserver name>]** - Owning Vserver

Use this parameter with the name of a Vserver to display only jobs that are owned by that Vserver.

**[-name <text>]** - Name

---

Use this parameter to display information only about the jobs that match the job name you specify.

**[-description <text>]** - Description

Use this parameter to display information only about the jobs that match the description you specify.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Use this parameter to display information only about the jobs that match the priority you specify.

**[-node <nodename>]** - Node

Use this parameter to display information only about the jobs that are associated with the node you specify.

**[-affinity {Cluster|Node}]** - Affinity

Use this parameter with an affinity value to display only jobs that match the affinity you specify.

**[-schedule <job\_schedule>]** - Schedule

Use this parameter to display information only about the jobs that run on the schedule you specify.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Use this parameter to display information only about the jobs that match the queue time you specify.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Use this parameter to display information only about the jobs that match the start time you specify.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Use this parameter to display information only about the jobs that match the end time you specify.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Use this parameter to display information only about the jobs that match the final timeout time you specify.

**[-restarted {true|false}]** - Restarted?

Use this parameter to display information only about the jobs that match the restart value you specify.

---

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Use this parameter to display information only about the jobs that match the job state you specify.

**[-code <integer>]** - Status Code

Use this parameter to display information only about the jobs that match the status code you specify.

**[-completion <text>]** - Completion String

Use this parameter to display information only about the jobs that match the completion text you specify.

**[-jobtype <text>]** - Job Type

Use this parameter to display information only about the jobs that match the job type you specify.

**[-category <text>]** - Job Category

Use this parameter to display information only about the jobs that match the job category you specify.

**[-uuid <UUID>]** - UUID

Use this parameter to display information only about the jobs that match the UUID you specify.

**[-username <text>]** - User Name

Use this parameter with a username to display only jobs that are associated with the user you specify.

## Examples

The following example displays information about all cluster-affiliated jobs:

```
cluster1::> job show-cluster
Job ID Name                Owning      Node      State
-----
305    Auto_Mirror            node-vserver
6202   mirror-03_10            node-vserver
6203   Descr:Auto mirror
      mirror-04_10        node-vserver
6204   Descr:Auto mirror
      mirror-01_10        node-vserver
6205   Descr:Auto mirror
      mirror-02_10        node-vserver
6206   Descr:Auto mirror
      mirror-05_10        node-vserver
```

---

Descr:Auto mirror	-	Queued
-------------------	---	--------



---

## job show-completed

Display a list of completed jobs

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

### Description

The `job show-completed` command displays information about completed jobs. The command output depends on the parameters you specify with the command. If you do not use any parameters, the command displays information about all completed jobs.

To display detailed information about a specific job, run the command with the `-id` parameter. The detailed view includes all of the default information plus additional items.

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about jobs running on a specific node, run the command with the `-node` parameter.

### Parameters

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

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

| **[-instance ]** }

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

**[-id <integer>]** - Job ID

Use this parameter to display information only about the jobs that match the ID or range of IDs you specify.

**[-vserver <vserver name>]** - Owning Vserver

Use this parameter with the name of a Vserver to display only jobs that are owned by that Vserver.

**[-name <text>]** - Name

Use this parameter to display information only about the jobs that match the name you specify.

---

**[-description <text>]** - Description

Use this parameter to display information only about the jobs that match the description you specify.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Use this parameter to display information only about the jobs that match the priority you specify.

**[-node <nodename>]** - Node

Use this parameter to display information only about the jobs that are associated with the node you specify.

**[-affinity {Cluster|Node}]** - Affinity

Use this parameter with an affinity value to display only jobs that match the affinity you specify.

**[-schedule <job\_schedule>]** - Schedule

If you use this parameter, the command displays information only about the jobs that have the schedule you specify.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

If you use this parameter, the command displays information only about the jobs that have the queue time you specify.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Use this parameter to display information only about the jobs that have the start time you specify.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Use this parameter to display information only about the jobs that have the end time you specify.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Use this parameter to display information only about the jobs that time out at the time you specify.

**[-restarted {true|false}]** - Restarted?

Use this parameter to display information only about the jobs that match the restart value you specify.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

---

Use this parameter to display information only about the jobs that match the job state you specify.

**[-code <integer>]** - Status Code

Use this parameter to display information only about the jobs that match the status code you specify.

**[-completion <text>]** - Completion String

Use this parameter to display information only about the jobs that match the completion text you specify.

**[-jobtype <text>]** - Job Type

Use this parameter to display information only about the jobs that match the job type you specify.

**[-category <text>]** - Job Category

Use this parameter to display information only about the jobs that match the job category you specify.

**[-uuid <UUID>]** - UUID

Use this parameter to display information only about the jobs that match the UUID you specify.

**[-username <text>]** - User Name

Use this parameter with a username to display only jobs that are associated with that user.

## Examples

The following example displays information about all completed jobs:

```
node::> job show-completed
Job ID Name          Owning Vserver End Time      Code      Completion String
-----
305      Auto_Mirror        node-vserver 10/10 08:07:05 0          Succeeded
6202     mirror-03_10       node-vserver 10/10 11:10:07 0
6203     mirror-04_10       node-vserver 10/10 12:10:09 0
6204     mirror-01_10       node-vserver 10/10 09:10:03 0
6205     mirror-02_10       node-vserver 10/10 10:10:08 0
6206     mirror-05_10       node-vserver 10/10 05:10:04 0
```

---

## job show

Display a list of jobs

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

### Description

The `job show` command displays information about jobs. By default, the command displays information about all current jobs.

To display detailed information about a specific job, run the command with the `-id` parameter.

You can specify additional parameters to select information that matches the values you specify for those parameters. For example, to display information only about jobs running on a specific node, run the command with the `-node` parameter.

### Parameters

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

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

| **[-inprogress]** ]

Displays the job ID, the job name, the owning Vserver, and the progress of the job.

| **[-jobstate]** ]

Displays information about each job's state, including the queue state, whether the job was restarted, and when the job has completely timed out.

| **[-sched]** ]

Displays the job ID, the job name, the owning Vserver, and the schedule on which the job runs.

| **[-times]** ]

Displays the job ID, the job name, the owning Vserver, the time when the job was last queued, the time when the job was last started, and the time when the job most recently ended.

---

| **[-type]**

Displays the job ID, the job name, the job type, and the job category.

| **[-jobuuid]** (privilege: advanced)

Displays the job ID, the job name, the owning Vserver, and the job UUID.

| **[-instance]** }

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

**[-id <integer>]** - Job ID

Selects the jobs that match the ID or range of IDs that you specify.

**[-vserver <vserver name>]** - Owning Vserver

Selects jobs that are owned by the specified Vserver.

**[-name <text>]** - Name

Selects the jobs that match this parameter value.

**[-description <text>]** - Description

Selects the jobs that match this parameter value.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Selects the jobs that match this parameter value.

**[-node <nodename>]** - Node

Selects the jobs that match this parameter value.

**[-affinity {Cluster|Node}]** - Affinity

Selects the jobs that match this parameter value.

**[-schedule <job\_schedule>]** - Schedule

Selects the jobs that match this parameter value.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Selects the jobs that match this parameter value.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Selects the jobs that match this parameter value.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Selects the jobs that match this parameter value.

---

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Selects the jobs that match this parameter value.

**[-restarted {true|false}]** - Restarted?

Selects the jobs that match this parameter value.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Selects the jobs that match this parameter value.

**[-code <integer>]** - Status Code

Selects the jobs that match this parameter value.

**[-completion <text>]** - Completion String

Selects the jobs that match this parameter value.

**[-jobtype <text>]** - Job Type

Selects the jobs that match this parameter value.

**[-category <text>]** - Job Category

Selects the jobs that match this parameter value.

**[-uuid <UUID>]** - UUID (privilege: advanced)

Selects the jobs that match this parameter value.

**[-progress <text>]** - Execution Progress

Selects the jobs that match this parameter value.

**[-username <text>]** - User Name

Selects the jobs that match this parameter value.

## Examples

The following example displays information about all jobs on the node named node1:

```
cluster1::> job show -node node1
Job ID Name                               Owning      Node      State
-----
308114 mirror-daily-3587206                node-vserver node1      Running
      Descr:Auto-replicate to 1 mirror(s)
308115 mirror-daily-3618985                node-vserver node1      Running
      Descr:Auto-replicate to 1 mirror(s)
308116 mirror-daily-3619010                node-vserver node1      Queued
```

---

```
308117 Descr:Auto-replicate to 1 mirror(s)
        mirror-daily-3749547
              node-vserver
                    node1      Queued
        Descr:Auto-replicate to 1 mirror(s)
4 entries were displayed.
```

---

## job stop

Stop a job

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

### Description

The `job stop` command stops a running job. A stopped job cannot be resumed. Use the `job pause` command to pause a job so that you can later resume it. Use the `job show` command to view a list of running jobs.

### Parameters

**-id** <integer> - Job ID

The numeric ID of the job to stop. A job ID is a positive integer.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example stops the job that has ID 101:

```
cluster1::> job stop -id 101
```

### See Also

`job pause` `job show`



---

## job unclaim

Unclaim a cluster job

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

### Description

The `job unclaim` command causes a cluster-affiliated job that is owned by an unavailable node to be unclaimed by that node. Another node in the cluster can then take ownership of the job. Use the `job show-cluster` command to obtain a list of cluster-affiliated jobs.

### Parameters

**-id** <integer> - Job ID

Use this parameter to specify the ID number of the job to unclaim.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example shows how to unclaim the cluster-affiliated job with the ID 27 that is owned by the Vserver `vs1`:

```
cluster1::*> job unclaim -vserver vs1 -id 27
```

### See Also

`job show-cluster`

---

## job watch-progress

Watch the progress of a job

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

### Description

The `job watch-progress` command displays the progress of a job, and periodically updates that display. You can specify the frequency of the updates.

### Parameters

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the job to monitor.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

**[-interval <integer>]** - Refresh Interval (seconds)

Use this parameter to specify the number of seconds between updates.

### Examples

The following example show how to monitor the progress of the job that has ID 222 on Vserver `vs0`. The progress display updates every 3 seconds.

```
cluster1::> job watch-progress -vserver vs0 -id 222 -interval 3
```

## job history show

Display a history of jobs

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

### Description

The `job history show` command displays a history of completed jobs with newer entries displayed first. You can specify optional parameters to select information about job history items that match only those parameters. For example, to display information

---

about jobs that were completed on February 27 at noon, run the command with `-endtime "02/27 12:00:00"`.

## Parameters

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

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

**| [-instance ] }**

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

**[-node {<nodename>|local}]** - Node

Selects the completed jobs that match this parameter value.

**[-record <Sequence Number>]** - Record ID

Selects the completed jobs that match the record ID or range of record IDs you specify. Note that record IDs are unique for each node, not for the cluster as a whole. As a result, there can be two records with the same record ID within the cluster.

**[-vserver <vserver name>]** - Owning Vserver

Selects the completed jobs that are owned by the Vserver you specify.

**[-id <integer>]** - Job ID

Selects the completed jobs that match this parameter value.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Selects jobs that completed at the time you specify. This parameter is most useful when used with a range of times.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Selects completed jobs that were started at the time you specify. This parameter is most useful when used with a range of times.

**[-name <text>]** - Name

Selects the completed jobs that match this parameter value.

**[-description <text>]** - Description

Selects the completed jobs that match this parameter value.

**[-code <integer>]** - Status Code

---

Selects the completed jobs that match this parameter value. Each job defines its own status codes. The completion text is more informative, but support technicians may request this numeric code.

**[-progress <text>]** - Progress String

Selects the completed jobs that match this parameter value.

**[-completion <text>]** - Completion String

Selects the completed jobs that match this parameter value.

**[-jobuuid <UUID>]** - Job UUID (privilege: advanced)

Selects the completed jobs that match this parameter value.

**[-event-type {Idle|Running|Succeeded|Failed|Paused|Stopped|Deleted|Error}]** - Event Type

Selects the completed jobs that match this parameter value.

**[-event-time <MM/DD HH:MM:SS>]** - Event Time

Selects the completed jobs that match this parameter value. This parameter is most useful when used with a range of times.

**[-error-code <integer>]** - Job Manager Error Code

Selects the completed jobs that match this parameter value.

**[-error-text <text>]** - Job Manager Error Text

Selects the completed jobs that match this parameter value.

**[-username <text>]** - User Name

Selects the completed jobs that match this parameter value.

## Examples

The following example displays information about all completed jobs:

```
cluster1::> job history show
```

Time	Node	Owning Vserver	Name	Event	Job ID
08/23 08:58:24	node1	node1-vs	Vol Create	Succeeded	76
Description: Create testvol					
Completion: Successful					
08/23 08:58:22	node1	node1-vs	Vol Create	Running	76
Description: Create testvol					
08/22 08:16:36	node1	node1-vs	CLUSTER BACKUP AUTO	weekly Succeeded	4
Description: Cluster Backup Job					
08/22 08:15:49	node1	node1-vs	CLUSTER BACKUP AUTO	weekly Running	4
Description: Cluster Backup Job					
08/22 08:15:08	node1	node1-vs	CLUSTER BACKUP AUTO	weekly Idle	4
Description: Cluster Backup Job					

---

```
08/22 08:15:03 node1          node1-vs  CLUSTER BACKUP AUTO weekly
                                Running
Description: Cluster Backup Job
6 entries were displayed.
```

The following example shows how to use a range with the "endtime" parameter to select only the events that ended between 8:15 and 8:16 on August 22nd.

```
cluster1::> job history show -endtime "08/22 08:15:00".. "08/22 08:16:00"
Time           Node           Owning  Name           Event           Job ID
-----
08/22 08:15:49 node1          node1-vs  CLUSTER BACKUP AUTO weekly
                                Running
Description: Cluster Backup Job
08/22 08:15:08 node1          node1-vs  CLUSTER BACKUP AUTO weekly
                                Idle
Description: Cluster Backup Job
08/22 08:15:03 node1          node1-vs  CLUSTER BACKUP AUTO weekly
                                Running
Description: Cluster Backup Job
3 entries were displayed.
```

---

## job initstate show

Display init state for job managers

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

### Description

The `job initstate show` command displays information about the initialization states of job-manager processes.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the nodes that match this parameter value.

[-**process** <process\_name>] - Process Name

Selects the nodes that match this parameter value.

[-**initialized** {true|false}] - Initialized?

Selects the nodes that match this parameter value (`true` means initialized; `false` means not initialized).

[-**cache-root** <text>] - Cache Root

Selects the nodes that match this parameter value.

[-**siteid** <UUID>] - Site ID

Selects the nodes that match this parameter value.

[-**hp-threads** <integer>] - High Priority Threads

Selects the nodes that have the number of high-priority threads you specify.

---

**[-mp-threads <integer>]** - Medium Priority Threads

Selects the nodes that have the number of medium-priority threads you specify.

**[-lp-threads <integer>]** - Low Priority Threads

Selects the nodes that have the number of low-priority threads you specify.

**[-tx-interval <integer>]** - Transaction Interval

Selects the nodes that have the number of seconds you specify as their transaction interval.

**[-initmsg <text>]** - Initialization Message

Selects the nodes that match this parameter value.

**[-thread-initmsg <text>]** - Thread Initialization Message

Selects the nodes that match this parameter value. The thread initialization message contains information about thread status. If there is no information to communicate, this message is empty.

**[-recovery-enabled {true|false}]** - Job Failover Enabled?

Selects the nodes that match this parameter value (`true` means enabled, `false` means not enabled).

**[-ex-threads <integer>]** - Exclusive Priority Threads

Selects the nodes that match this parameter value.

## Examples

The following example shows how to display general job-manager initialization-state information for a cluster.

```
cluster1::*> job initstate show
```

Node	Process	Init?	HP Thr	MP Thr	LP Thr	EX Thr	TX Int	Failover?
node1	mgwd	true	2	3	5	8	300	true
node2	mgwd	true	2	3	5	8	300	true

2 entries were displayed.

The following example shows how to display detailed job-manager initialization-state information for a node named `node0`.

```
cluster1::*> job initstate show -instance -node node0
```

```
Node: node0
Process Name: mgwd
Initialized?: true
Cache Root: /mroot/jm_cache
Site ID: 824e8f7d-f49-1d9-84af-00423b7352
High Priority Threads: 2
Medium Priority Threads: 3
Low Priority Threads: 5
Transaction Interval: 300
Initialization Message: Initialized
```

---

```
Are Threads Running?: -  
Job Failover Enabled?: true  
Exclusive Priority Threads: 8
```



---

## job private delete

Delete a job

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

### Description

The `job private delete` command deletes a private job. Private jobs are affiliated with a specific node and do not use any cluster facilities, such as the replicated database.

If you use this command on a job that does not support the delete operation, the command returns an error message.

Use the `job private show` command to view a list of private jobs that can be deleted.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node with which the private job is associated.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the private job to be deleted. A job ID is a positive integer.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example shows how to delete the job that has ID 273 from the node named `node2`:

```
cluster1::*> job private delete -node node2 -id 273
```

### See Also

`job private show`

---

## job private pause

Pause a job

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

### Description

The `job private pause` command pauses a private job. Private jobs are affiliated with a specific node and do not use any cluster facilities, such as the replicated database.

If you use this command to pause a job that does not support it, the command returns an error message.

Use the `job private resume` command to resume a paused private job.

Use the `job private show` command to view a list of private jobs.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node with which the private job is associated.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the paused private job to be paused. A job ID is a positive integer.

**-vserver** <vserver name> - Owning Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example pauses the private job that has ID 99 on the node `node1`:

```
cluster1::*> jobs private pause -node node1 -id 99
```

### See Also

`job private resume`   `job private show`

---

## job private resume

Resume a job

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

### Description

The `job private resume` command resumes a private job that was paused by using the `job private pause` command. Private jobs are affiliated with a specific node and do not use any cluster facilities, such as the replicated database.

Use the `job private show` command to view a list of paused private jobs that can be resumed.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node with which the paused private job is associated.

**-id** <integer> - Job ID

Use this parameter to specify the numeric ID of the paused private job to be resumed. A job ID is a positive integer.

**-vserver** <vserver name> - Owning Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example resumes the paused private job that has ID 99 on a node named `node2`:

```
cluster1::*> job private resume -node node2 -id 99
```

### See Also

`job private pause`   `job private show`

---

## job private show-completed

Display a list of completed jobs

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

### Description

The `job private show-completed` command displays information about completed private jobs. Private jobs are affiliated with a specific node and do not use any cluster facilities, such as the replicated database.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Use this parameter to display information only about completed jobs that are associated with the node you specify.

[-id <integer>] - Job ID

Use this parameter to display information only about completed jobs that have the ID you specify.

[-vserver <vserver name>] - Owning Vserver

Use this parameter to display only completed jobs that are owned by the Vserver you specify.

[-name <text>] - Name

Use this parameter to display information only about completed jobs that have the name you specify.

[-description <text>] - Description

---

Use this parameter to display information only about completed jobs that have the description you specify.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Use this parameter to display information only about completed jobs that have the priority you specify.

**[-schedule <job\_schedule>]** - Schedule

Use this parameter to display information only about completed jobs that have the schedule you specify.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Use this parameter to display information only about completed jobs that have the queue time you specify.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Use this parameter to display information only about completed jobs that have the start time you specify.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Use this parameter to display information only about completed jobs that have the end time you specify.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Use this parameter to display information only about completed jobs that have the final timeout time you specify.

**[-restarted {true|false}]** - Restarted?

Use this parameter to display information only about completed jobs that have the restart value you specify.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Use this parameter to display information only about completed jobs that have the job state you specify.

**[-code <integer>]** - Status Code

Use this parameter to display information only about completed jobs that have the status code you specify.

**[-completion <text>]** - Completion String

---

Use this parameter to display information only about completed jobs that have the completion text you specify.

**[-jobtype <text>]** - Job Type

Use this parameter to display information only about completed jobs that have the job type you specify.

**[-category <text>]** - Job Category

Use this parameter to display information only about completed jobs that have the job category you specify.

**[-uuid <UUID>]** - UUID

Use this parameter to display information only about completed jobs that have the UUID you specify.

**[-username <text>]** - User Name

Use this parameter to display information only about completed jobs that are associated with the user you specify.

### Examples

The following example shows how to display information about all completed private jobs on the node named `node1`:

```
cluster1::*> job private show-completed -node node1
Node: node1
```

Job ID	Name	Owning Vserver	End Time	Code	Completion String
1	sync task	node1	02/17 15:03:23	0	
2	load_balancing	node1	02/17 16:29:28	0	DONE_VIF_STATS
3	snap-hourly	node1	02/17 16:05:00	0	
4	snap-daily	node1	02/17 00:10:00	0	
5	snap-weekly	node1	02/13 00:15:00	0	
8	Cross-Cluster Manager	node1	02/17 16:27:27	0	complete
9	reconcile service policy	node1	02/17 15:03:12	0	

7 entries were displayed.

---

## job private show

Display a list of jobs

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

### Description

The `job private show` command displays information about private jobs. Private jobs are affiliated with a specific node and do not use any cluster facilities, such as the replicated database.

### Parameters

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

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

| [-inprogress ]

Displays the job ID, name, owning Vserver, and progress of each private job.

| [-jobstate ]

Displays information about each private job's state, including the queue state, whether the job was restarted, and when the job has timed out.

| [-jobuuid ]

Displays the ID, name, owning Vserver, and UUID of each private job.

| [-sched ]

Displays the job ID, name, owning Vserver, and run schedule of each private job.

| [-times ]

Displays the queue time, start time, and end time of each private job.

| [-type ]

Displays the type and category of each private job.

| [-instance ] }

---

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

**[-node <nodename>|local]** - Node

Selects the private jobs that match this parameter value. .

**[-id <integer>]** - Job ID

Selects the private jobs that match the ID or range of IDs that you specify.

**[-vserver <vserver name>]** - Owning Vserver

Selects the private jobs that match this parameter value.

**[-name <text>]** - Name

Selects the private jobs that match this parameter value.

**[-description <text>]** - Description

Selects the private jobs that match this parameter value.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Selects the private jobs that match this parameter value.

**[-schedule <job\_schedule>]** - Schedule

Selects the private jobs that match this parameter value.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Selects the private jobs that match this parameter value.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

Selects the private jobs that match this parameter value.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Selects the private jobs that match this parameter value.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Selects the private jobs that match this parameter value.

**[-restarted {true|false}]** - Restarted?

Selects the private jobs that match this parameter value.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Selects the private jobs that match this parameter value.



---

**[-code <integer>]** - Status Code

Selects the private jobs that match this parameter value.

**[-completion <text>]** - Completion String

Selects the private jobs that match this parameter value.

**[-jobtype <text>]** - Job Type

Selects the private jobs that match this parameter value.

**[-category <text>]** - Job Category

Selects the private jobs that match this parameter value.

**[-uuid <UUID>]** - UUID

Selects the private jobs that match this parameter value.

**[-progress <text>]** - Execution Progress

Selects the private jobs that match this parameter value.

**[-username <text>]** - User Name

Selects the private jobs that match this parameter value.

## Examples

The following example displays information about all private jobs on the local node:

```
cluster1::*> job private show -node local
Node: node1

```

Job ID	Name	Owning Vserver	State
3	snap-hourly	cluster1	Queued
	Description: Auto-Snapshot		
4	snap-daily	cluster1	Queued
	Description: Auto-Snapshot		
5	snap-weekly	cluster1	Queued
	Description: Auto-Snapshot		
6	sync task	cluster1	Queued
	Description: sync task		
7	ldap-certs	cluster1	Queued
	Description: ldap resync		

```
5 entries were displayed.
```

---

## job private stop

Stop a job

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

### Description

The `job private stop` command stops a running private job. A private job is a job that is associated with a specific node and does not use cluster facilities. A stopped job cannot be restarted.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the job is running.

**-id** <integer> - Job ID

This specifies the numeric ID of the job that is to be stopped.

**-vserver** <vserver name> - Owing Vserver

Use this parameter to specify the name of the Vserver that owns the job.

### Examples

The following example stops a private job with the ID 416 on a node named node0:

```
cluster1::*> job private stop -node node0 -id 416
```

## job private watch-progress

Watch the progress of a job

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

### Description

The `job private watch-progress` command displays and periodically updates the progress of a private job. A private job is a job that is associated with a specific

---

node and does not use cluster facilities. You can specify the frequency of the progress updates.

## Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the job is running.

**-id** <integer> - Job ID

This specifies the numeric ID of the job whose progress is to be monitored.

**-vserver** <vserver name> - Owning Vserver

Use this parameter to specify the Vserver with which the paused private job is associated. Use this parameter to specify the name of the Vserver that owns the job.

**[-interval <integer>]** - Refresh Interval (seconds)

This optionally specifies, in seconds, the frequency of the updates.

## Examples

The following example monitors the progress of the private job that has ID 127 on a node named node1. The progress is updated every 2 seconds.

```
cluster1::*> job private watch-progress -node node1 -id 127 -interval 2
Queued
```

## job schedule delete

Delete a schedule

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

## Description

The `job schedule delete` command deletes a schedule. Use the `job schedule show` command to display all current schedules.

You cannot delete any schedules that are in use by jobs. Use the `job schedule show-jobs` command to display jobs by schedule.

You cannot delete any schedules that are referenced by:

- Volume Snapshot copy policy entries
- SnapMirror entries

- 
- antivirus on-demand entries
  - SIS policy entries
  - configuration backup settings

You must remove all references to a schedule before you can delete it. If you attempt to delete a schedule that is referenced, an error message will list which entries reference the schedule you want to delete. Use the `show` command for each of the items listed by the error message to display which entries reference the schedule. You may need to use the `-instance` parameter to display more detail.

## Parameters

**-name** <text> - Schedule Name

Use this parameter with the name of an existing schedule to specify the schedule you want to delete.

## Examples

The following example deletes a schedule named `overnightbackup`:

```
cluster1::> job schedule delete -name overnightbackup
```

## See Also

`job schedule show`   `job schedule show-jobs`

---

## job schedule show-jobs

Display the list of jobs by schedule

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

### Description

The `job schedule show-jobs` command displays information about jobs that are associated with schedules.

### Parameters

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

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

| [-instance ] }

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

[-name <text>] - Schedule Name

Use this parameter to display information only about the jobs that are associated with the schedule you specify.

[-affinity {Cluster|Node}] - Cluster / Node

Use this parameter to display information only about the jobs that match the affinity value you specify.

[-owner <text>] - Owner

Use this parameter to display information only about the jobs that are owned by the nodes you specify.

[-jobid <integer>] - ID

Use this parameter to display information only about the jobs that match the ID or range of IDs that you specify.

[-jobname <text>] - Job Name

---

Use this parameter to display information only about the jobs that match the name you specify.

### Examples

The following example shows information about schedules that are associated with jobs:

```
cluster1::> job schedule show-jobs
Name          Type      Owner          Job ID      Job Name
-----
hourly        Cluster  -              98644      mirror-hourly
weeklylog     Node     node0          1501      log-rotation
weeklylog     Node     node1          1498      log-rotation
weeklylog     Node     node2          1499      log-rotation
weeklylog     Node     node3          1500      log-rotation
5 entries were displayed.
```

---

## job schedule show

Display a list of available schedules

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

### Description

The `job schedule show` command displays information about schedules.

### Parameters

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

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

| [-instance ] }

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

**[-name <text>]** - Schedule Name

Selects the schedules that match this parameter value.

**[-type {cron|interval|builtin}]** - Schedule Type

Selects the schedules that match this parameter value.

**[-description <text>]** - Description

Selects the schedules that match this parameter value.

### Examples

The following example displays information about all cron schedules:

```
cluster1::> job schedule show -type cron
Name      Type      Description
-----
5min      cron      @:00,:05,:10,:15,:20,:25,:30,:35,:40,:45,:50,:55
daily     cron      @0:10
hourly    cron      @:05
midnightcron cron      Sun@0:00
weekendcron cron      Sun,Sat@3:15
```

---

## job schedule cron create

Create a cron schedule

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

### Description

The `job schedule cron create` command creates a cron schedule. A cron schedule, like a UNIX cron job, runs at a specified time. You can also specify months, days of the month, or days of the week on which the schedule will run.

If you specify values for both days of the month and days of the week, they are considered independently. For example, a cron schedule with the day specification Friday, 13 runs every Friday and on the 13th day of each month, not just on every Friday the 13th.

### Parameters

**-name** <text> - Name

Use this parameter to specify the name of the interval schedule that you want to create.

**[-month** <cron\_month>, ...] - Month

Use this parameter to specify months in which the schedule runs. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, and all. Specify "all" to run the schedule every month.

**[-dayofweek** <cron\_dayofweek>, ...] - Day of Week

Use this parameter to specify days of the week on which the schedule runs. Valid values are Sunday, Monday, Tuesday, Thursday, Friday, and Saturday, and all. Specify "all" to run the schedule every day.

**[-day** <cron\_dayofmonth>, ...] - Day

Use this parameter to specify days of the month on which the schedule runs. Valid values range from 1 to 31.

**[-hour** <cron\_hour>, ...] - Hour

Use this parameter to specify the hours value of the time of day at which the schedule runs. Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specify "all" to run the schedule every hour.



---

**-minute** <cron\_minute>, ... - Minute

Use this parameter to specify the minutes portion of the time of day at which the schedule runs. Valid values range from 0 to 59.

## Examples

The following example creates a cron schedule named `weekendcron` that runs on weekend days (Saturday and Sunday) at 3:00 a.m.

```
cluster1::> job schedule cron create -name weekendcron -dayofweek "Saturday,  
Sunday" -hour 3 -minute 0
```

## job schedule cron delete

Delete a cron schedule

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

## Description

The `job schedule cron delete` command deletes a cron schedule. Use the `job schedule cron show` command to display all current cron schedules.

You cannot delete any cron schedules that are associated with jobs. Use the `job schedule show-jobs` command to display jobs by schedule.

## Parameters

**-name** <text> - Name

Use this parameter with the name of an existing cron schedule to specify the cron schedule that you want to delete.

## Examples

The following example deletes a cron schedule named `midnightcron`:

```
cluster1::> job schedule cron delete -name midnightcron
```

## See Also

`job schedule cron show` `job schedule show-jobs`

---

## job schedule cron modify

Modify a cron schedule

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

### Description

The `job schedule cron modify` command modifies a cron schedule. A cron schedule, like a UNIX cron job, runs at a specified time. You can also specify months, days of the month, or days of the week on which the schedule runs. Use the `job schedule cron show` command to display all current cron schedules. See the documentation for `job schedule cron show` for more information about how cron schedules work.

Modifying one parameter of a cron schedule does not affect the other parameters. For example, if cron schedule is set to run at 3:15 AM, and you modify the "hour" parameter to 4, the schedule's new time will be 4:15am. To clear a parameter of the schedule's interval, you must explicitly set that portion to "0" or "-". Some parameters can also be set to "all".

### Parameters

**-name** <text> - Name

Use this parameter with the name of an existing cron schedule to specify the cron schedule you want to modify.

**[-month** <cron\_month>, ...] - Month

Use this parameter to specify a new "month" value for the cron schedule. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, or all. Specify "all" to run the schedule every month.

**[-dayofweek** <cron\_dayofweek>, ...] - Day of Week

Use this parameter to specify a new "day of week" value for the cron schedule. Valid values include Sunday, Monday, Tuesday, Thursday, Friday, Saturday, or all. Specify "all" to run the schedule every day.

**[-day** <cron\_dayofmonth>, ...] - Day

Use this parameter to specify a new "day of month" value for the cron schedule. Valid values range from 1 to 31.

---

**[-hour <cron\_hour>, ...]** - Hour

Use this parameter to specify a new "hour of the day" value for the cron schedule. Valid values range from 0 (midnight) to 23 (11:00 p.m.), Specify "all" to run the schedule every hour.

**[-minute <cron\_minute>, ...]** - Minute

Use this parameter to specify a new "minute of the hour" value for the cron schedule. Valid values range from 0 to 59.

## Examples

The following example modifies a cron schedule named weekendcron so that it runs at 3:15 a.m.:

```
cluster1::> job schedule cron modify -name weekendcron -hour 3 -minute 15
```

## See Also

`job schedule cron show`

---

## job schedule cron show

Show cron schedules

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

### Description

The `job schedule cron show` command displays information about cron schedules. A cron schedule runs a job at a specified time on specified days.

### Parameters

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

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

| **[-instance ]** }

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

**[-name <text>]** - Name

Selects the cron schedules that match this parameter value.

**[-month <cron\_month>, ...]** - Month

Selects the cron schedules that match this parameter value. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, or all.

**[-dayofweek <cron\_dayofweek>, ...]** - Day of Week

Selects the cron schedules that match this parameter value. Valid values include Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or all.

**[-day <cron\_dayofmonth>, ...]** - Day

Selects the cron schedules that match this parameter value. Valid values range from 1 to 31.

**[-hour <cron\_hour>, ...]** - Hour

Selects the cron schedules that match this parameter value.

---

**[-minute <cron\_minute>, ...]** - Minute

Selects the cron schedules that match the minute or range of minutes that you specify.

**[-description <text>]** - Description

Selects the cron schedules that match this parameter value.

## Examples

The following example displays information about all current cron schedules:

```
cluster1::> job schedule cron show
```

Name	Description
weekendcron	Sun,Sat@3:15

The following example displays information about the cron schedule named weekendcron:

```
cluster1::> job schedule cron show -name weekendcron
```

```
      Name: weekendcron
      Month: -
Day of Week: Sunday, Saturday
      Day: -
      Hour: 3
      Minute: 15
Description: Sun,Sat@3:15
```

---

## job schedule interval create

Create a schedule that runs on an interval

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

### Description

The `job schedule interval create` creates an interval schedule. An interval schedule runs jobs at specified intervals after the previous job finishes. For instance, if a job uses an interval schedule of 12 hours and takes 30 minutes to complete, the job runs at the following times:

- Day one at 8:00 a.m. (the job's initial run)
- Day one at 8:30 p.m.
- Day two at 9:00 a.m.
- Day two at 9:30 p.m.

Each of the numerical parameters of the interval must be a whole number. These parameters can be used individually, or combined to define complex time values. For example, use a value of 1 day, 12 hours to create an interval of 1.5 days.

Large parameter values are converted into larger units. For example, if you create a schedule with an interval of 36 hours, the `job schedule interval show` command will display it with an interval of 1 day 12 hours.

### Parameters

**-name** <text> - Name

Use this parameter to specify the name of the interval schedule you want to create.

**[-days** <integer>] - Days

Use this parameter to specify the "days" portion of the schedule's interval. A day is one calendar day.

**[-hours** <integer>] - Hours

Use this parameter to specify the "hours" portion of the schedule's interval.

**[-minutes** <integer>] - Minutes

---

Use this parameter to specify the "minutes" portion of the schedule's interval.

**[-seconds <integer>]** - Seconds

Use this parameter to specify the "seconds" portion of the schedule's interval.

## Examples

The following example creates an interval schedule named `rollingdaily` that runs six hours after the completion of the previous occurrence of the job:

```
cluster1::> job schedule interval create -name rollingdaily -hours 6
```

## See Also

`job schedule interval show`

---

## job schedule interval delete

Delete an interval schedule

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

### Description

The `job schedule interval delete` command deletes an interval schedule. Use the `job schedule interval show` command to display all current interval schedules.

You cannot delete interval schedules that are currently being run. Use the `job schedule show-jobs` command to display jobs by schedule.

### Parameters

**-name** <text> - Name

Use this parameter with the name of an existing interval schedule to specify the interval schedule you want to delete.

### Examples

The following example deletes an interval schedule named `rollingdaily`:

```
cluster1::> job schedule interval delete -name rollingdaily
```

### See Also

`job schedule interval show` `job schedule show-jobs`



---

## job schedule interval modify

Modify an interval schedule

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

### Description

The `job schedule interval modify` command modifies an interval schedule. An interval schedule runs jobs at a specified interval after the previous job finishes. Use the `job schedule interval show` command to display all current interval schedules. See the documentation of `job schedule interval show` for more information on how interval schedules work.

Modifying one parameter of a schedule's interval does not affect the other parameters. For example, if a schedule's interval is 1 day 12 hours, and you modify the "hours" parameter to 16, the schedule's new interval is 1 day 16 hours. To clear a parameter of the schedule's interval, you must explicitly set that parameter to "0" or "-".

### Parameters

**-name** <text> - Name

Use this parameter with the name of an existing interval schedule to specify the interval schedule you want to modify.

**[-days** <integer>] - Days

Use this parameter to specify a different "days" value for the schedule's interval.

**[-hours** <integer>] - Hours

Use this parameter to specify a different "hours" value for the schedule's interval.

**[-minutes** <integer>] - Minutes

Use this parameter to specify a different "minutes" value for the schedule's interval.

**[-seconds** <integer>] - Seconds

Use this parameter to specify a different "seconds" value for the schedule's interval.

### Examples

The following example sets the schedule named `rollingdaily` to run every eight hours:

```
cluster1::> job schedule interval modify -name rollingdaily -hours 8
```

---

## See Also

`job schedule interval show`

---

## job schedule interval show

Show interval schedules

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

### Description

The `job schedule interval show` command displays information about interval schedules.

### Parameters

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

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

| [-**instance** ] }

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

[-**name** <text>] - Name

Selects the interval schedules that match this parameter value.

[-**days** <integer>] - Days

Selects the interval schedules that match the day value or range of values you specify.

[-**hours** <integer>] - Hours

Selects the interval schedules that match the hour value or range of values you specify.

[-**minutes** <integer>] - Minutes

Selects the interval schedules that match the minute value or range of values you specify.

[-**seconds** <integer>] - Seconds

Selects the interval schedules that match the second value or range of values you specify.

[-**description** <text>] - Description

---

Selects the interval schedules that match the description you specify.

## Examples

The following example displays information about all interval schedules:

```
cluster1::> job schedule interval show
Name      Description
-----
rollingdaily      Every 8h
```

---

## lun create

Create a new LUN

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

### Description

This command creates a new empty LUN of a specific size. You cannot create a LUN in path that already exists. You must specify the LUN at a qtree root directory in the `lun_path`. A LUN can only exist at the root of a qtree. You can not create LUNs in the Vserver root volume.

You might find it useful to provide a meaningful path name for the LUN. For example, you might choose a name that describes how the LUN is used, such as the name of the application, the type of data that it stores, or the user accessing the data. Examples are `/vol/database/lun0`, `/vol/finance/lun1`, and `/vol/bill/lun2`.

For clustered storage system configurations, it is recommended that you distribute LUNs across the cluster.

When you can create a LUN, the size of the LUN could be larger than what you specified. The system generates a message if the size of the LUN is different from what you specified.

By default, when you create a LUN, it is online and it is space-reserved. Use the `lun offline` command to take a LUN offline. When you set space reserved to false, the LUN is thinly provisioned.

Note:

When you thinly provision a LUN, write operations to that LUN might fail due to insufficient disk space. As a result, the host application or operating system might crash.

Note:

When you create a LUN from a file, that file cannot be deleted without deleting the LUN itself.

Note:

This command is not supported for a Vserver with Infinite Volume.

---

## Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the new LUN. The LUN path cannot contain any files.

| **-volume** <volume name> - Volume Name

Specifies the volume that contains the new LUN.

[**-qtree** <text>] - Qtree Name

Specifies the qtree that contains the new LUN.

**-lun** <text> } - LUN Name

Specifies the new LUN name. A LUN name is a case-sensitive name and has the following requirements:

- Must contain one to 255 characters. Spaces are not allowed.
- Can contain the letters A through Z, a through z, numbers 0 through 9, hyphen (-), underscore (\_), right bracket (}), left bracket ({) and period (.).
- Must start with a letter or number.

{ **-size** | **-s** <size> - LUN Size

Specifies the size of the LUN in bytes. You can specify a one-character multiplier suffix:

- c (1 byte)
- w (2 bytes)
- B (512 bytes)
- k (1024 bytes)
- M (k\*k bytes)
- G (k\*m bytes)
- T (m\*m bytes)

| **-file-path** | **-f** <text> } - File Path

Creates a LUN using the file path as the source.

[**-prefix-size** | **-P** <size>] - Prefix Size (privilege: advanced)

---

Specifies the size of the prefix stream for the new LUN.

**-ostype** | **-t** <os\_enum> - OS Type

Specifies the OS type for the new LUN. The OS types are:

- aix - the LUN stores AIX data.
- hpux - the LUN stores HP-UX data.
- hyper\_v - the LUN stores Windows Server 2008 or Windows Server 2012 Hyper-V data
- linux - the LUN stores a Linux raw disk without a partition table.
- netware - the LUN stores NetWare data.
- openvms - the LUN store Open-VMS data
- solaris - the LUN stores Solaris raw disk in a single-slice partition.
- solaris\_efi - the LUN stores Solaris\_EFI data.
- vmware - the LUN stores VMware data
- windows - the LUN stores a raw disk type in a single-partition Windows disk using the Master Boot Record (MBR) partitioning style.
- windows\_gpt - the LUN stores Windows data using the GUID Partition Type (GPT) partitioning style.
- windows\_2008 - the LUN stores Windows data for Windows 2008 and 2012 systems.
- xen - the LUN stores Xen data

**[-space-reserve {enabled|disabled}]** - Space Reservation

Specifies whether the space reservation setting is enabled or disabled for the new LUN. If you set the parameter to enabled, the LUN is space-reserved. If you set the parameter to disable, the LUN is thinly provisioned. The default is enabled.

**[-class {regular|protocol-endpoint|vvol}]** - Class

Specifies the class of the new LUN. The class types are:

- regular - the LUN is for normal blocks protocol access. This is the default value.
- protocol-endpoint - the LUN is a vvol protocol endpoint.
- vvol - the LUN is a vvol data LUN.

**[-qos-policy-group <text>]** - QoS Policy Group

---

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

Note:

If you specify this parameter for a LUN that you want to create from a file and that file belongs to a QoS policy group, Data ONTAP adds the LUN to the specified policy group and removes the file from its policy group. Both the file and the LUN that you created from the file cannot belong to QoS policy groups.

## Examples

```
cluster1::> lun create -vserver vs1 -path /vol/vol1/lun1 -size 100M -ostype linux
```

Creates a 100MB LUN at path /vol/vol1/lun1 in Vserver vs1. The OS type is Linux, and the state is online.

## See Also

[lun offline](#)



---

## lun delete

Delete the LUN

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

### Description

This command deletes a LUN from a specified Vserver and volume. If the LUN is mapped and online, the force option is required to delete it.

If a LUN is mapped to an initiator group, you can unmap it by using the `lun unmap` command. If a LUN is online, you take it offline by using the `lun offline` command.

Note:

If you create a LUN from a file, you cannot remove the file while the LUN is linked to it. If you want to remove the file, you must first delete the LUN. This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the LUN you want to delete.

| **-volume** <volume name> - Volume Name

Specifies the volume that contains the LUN you want to delete.

[**-qtree** <text>] - Qtree Name

Specifies the qtree that contains the LUN you want to delete.

**-lun** <text> } - LUN Name

Specifies the LUN that you want to delete.

[**-force** | **-f** [true]] - Force Delete

Force deletion of an online LUN that is mapped to an initiator group.

---

## Examples

```
cluster1::> lun delete -vserver vs1 -path /vol/vol1/lun1
```

Deletes the LUN at path /vol/vol1/lun1 on Vserver vs1.

## See Also

`lun unmap` `lun offline`

---

## lun map

Maps a LUN to the initiators of an initiator group.

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

### Description

This command maps a LUN to all of the initiators in an initiator group (igroup). After you map the LUN, the LUN is visible to all initiators in the igroup.

Data ONTAP ensures that there are no LUN map conflicts whether the LUN is offline or online. A LUN map conflict is a mapping that would violate either of the following rules:

- Each LUN can be mapped to an initiator only once. A LUN can be mapped to multiple igroups as long as each igroup has a distinct set of initiators.
- LUN IDs must be unique such that every initiator has a unique ID for each LUN to which it is mapped. If you map a LUN to an igroup, the LUN ID for that mapping cannot be reused by any of the initiators in that igroup.

In order to determine if a LUN ID is valid for a mapping, Data ONTAP checks each initiator in the igroup to make sure that the LUN ID is not used for another mapping that includes that initiator.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the LUN that you want to map.

| **-volume** <volume name> - Volume Name

Specifies the volume that contains the LUN you want to map.

[**-qtree** <text>] - Qtree Name

---

Specifies the qtree that contains the LUN you want to map.

**-lun** <text> } - LUN Name

Specifies the LUN name that you want to map.

**-igroup** <text> - Initiator Group Name

Specifies the igroup that you want to map.

**[-lun-id <integer>]** - The LUN ID to assign for the mapping.

Specifies the LUN ID for the mapping. The LUN ID is specific to the mapping, not to the LUN itself. This is used by the initiators in the igroup as the Logical Unit Number for the initiator when accessing the storage.

## Examples

```
cluster1::> lun map -vserver vs1 -path /vol/vol1/lun1 -igroup ig1 -lun-id 8
```

Maps a LUN at /vol/vol1/lun1 on Vserver vs1 to the igroup ig1 with LUN ID 8.

---

## lun maxsize

Display the maximum possible size of a LUN on a given volume or qtree.

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

### Description

This command returns the maximum size of LUNs for different OS types in a volume or qtree. The command also includes possible maximum size for LUNs with Snapshots or without Snapshots. You can specify the path of the volume or qtree to determine the maximum size of a LUN that you want to create within that volume or qtree.

If you do not specify a path, the command returns the maximum LUN size for each OS type for all volumes and qtrees in a cluster.

The available space in a volume can change over time which means that the size reported by `lun maxsize` can change as well. In addition, the maximum LUN size allowed in a `lun resize` command may be less than the size reported by `lun maxsize`.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver Name

Specifies the Vserver.

{ [-path <qtree path>] - Volume or Qtree Path

Specifies the path of the root volume or qtree.

---

| **[-volume <volume name>]** - Volume Name

Specifies the volume that contains the LUN you want to get the maximum size for.

**[-qtree <qtree name>]** } - Qtree Name

Specifies the qtree that contains the LUN you want to get the maximum size for.

**[-ostype | -t <os\_enum\_ui>]** - OS Type

Specifies OS type of the LUN. The OS types are:

- aix - the LUN stores AIX data.
- hpux - the LUN stores HP-UX data.
- hyper\_v - the LUN stores Windows Server 2008 or Windows Server 2012 Hyper-V data
- linux - the LUN stores a Linux raw disk without a partition table.
- netware - the LUN stores NetWare data.
- openvms - the LUN store Open-VMS data
- solaris - the LUN stores Solaris raw disk in a single-slice partition.
- solaris\_efi - the LUN stores Solaris\_EFI data.
- vmware - the LUN stores VMware data
- windows - the LUN stores a raw disk type in a single-partition Windows disk using the Master Boot Record (MBR) partitioning style.
- windows\_gpt - the LUN stores Windows data using the GUID Partition Type (GPT) partitioning style.
- windows\_2008 - the LUN stores Windows data for Windows 2008 and 2012 systems.
- xen - the LUN stores Xen data

**[-complete-ss-reserve <size>]** - With Complete Snapshot Reserve

Shows the maximum size possible of a LUN if you have the complete Snapshot reserve enabled.

**[-ss-reserve <size>]** - With Snapshot Reserve

Shows the maximum size possible of a LUN if you have the Snapshot reserve enabled.

**[-without-ss-reserve <size>]** - Without Snapshot Reserve

Shows the maximum size possible of a LUN if you have no Snapshot reserve enabled.

---

# Examples

```
cluster1::> lun maxsize -volume vol0 -ostype netware
Virtual Server      Volume      Qtree      OS Type      Without SS Reserve  With SS Reserve  Complete SS Reserve
-----
vs0                 vol0         " "         netware      45MB              45MB              45MB
```

Displays the maximum size of a LUN for the OS type netware.

```
cluster1::> lun maxsize
Vserver      Volume      Qtree      OS Type      SS      Without SS Reserve  With SS Reserve  Complete SS Reserve
-----
vs1          voll         " "         hyper_v      172.6MB  172.6MB  172.6MB
vs1          voll         " "         windows_2008 172.6MB  172.6MB  172.6MB
vs1          voll         " "         windows_gpt  172.6MB  172.6MB  172.6MB
vs1          voll         " "         windows      172.6MB  172.6MB  172.6MB
vs1          voll         " "         linux        178MB    178MB    178MB
vs1          voll         " "         xen          178MB    178MB    178MB
vs1          voll         " "         solaris      178MB    178MB    178MB
vs1          voll         " "         solaris_efi  178MB    178MB    178MB
vs1          voll         " "         hpux         178MB    178MB    178MB
vs1          voll         " "         aix          178MB    178MB    178MB
vs1          voll         " "         netware      178MB    178MB    178MB
vs1          voll         " "         openvms      178MB    178MB    178MB
```

12 entries were displayed.

Displays the maximum size of LUNs for all OS types on volume vol1.

## See Also

[lun resize](#)

---

## lun modify

Modify a LUN

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

### Description

This command modifies LUN attributes. Because LUN modifications can result in data corruption or other problems, we recommend that you call technical support if you are unsure of the possible consequences of modifying a LUN.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path for the LUN you want to modify.

| **-volume** <volume name> - Volume Name

Specifies the volume for the LUN you want to modify.

**-qtree** <text> - Qtree Name

Specifies the qtree for the LUN you want to modify.

**-lun** <text> } - LUN Name

Specifies the name for the LUN you want to modify. A LUN name is a case-sensitive name and has the following requirements:

- Must contain one to 255 characters. Spaces are not allowed.
- Can contain the letters A through Z, a through z, numbers 0 through 9, hyphen (-), underscore (\_), right bracket (}), left bracket ({) and period (.).
- Must start with a letter or number.



---

**[-space-reserve {enabled|disabled}]** - Space Reservation

Specifies whether the space reservation setting is enabled or disabled for a LUN. If you set the parameter to `enabled`, the LUN is space-reserved. If you set the parameter to `disabled`, the LUN is thinly provisioned. The default is `enabled`.

**[-serial <text>]** - Serial Number

Specifies the serial number for the LUN you want to modify.

**[-comment <text>]** - Comment

Specifies the comment for the LUN you want to modify.

**[-space-allocation {enabled|disabled}]** - Space Allocation

Specifies whether space allocation is enabled or disabled for a LUN. If you set this parameter to `enabled`, space allocation is enabled and provisioning threshold events for the LUN are reported. If you set this parameter to `disabled`, space allocation is not enabled and provisioning threshold events for the LUN are not reported. The default is `disabled`.

**[-state <lunState\_enum>]** - State

Specifies the administrative state of a LUN. The options are:

- `online`
- `offline`

**{ [-device-legacy-id <integer>] - Device Legacy ID**

Specifies the device legacy ID for the LUN you want to modify.

**| [-device-binary-id <text>] - Device Binary ID**

Specifies the device binary ID for the LUN you want to modify.

**| [-clear-binary-id [true]] } - Clear Device Binary ID**

Clears the binary format of the optional device ID.

**{ [-device-text-id <text>] - Device Text ID**

Specifies the device text ID for the LUN you want to modify.

**| [-clear-text-id [true]] } - Clear Device Text ID**

Clears the text format of the optional device ID.

**[-qos-policy-group <text>] - QoS Policy Group**

This optionally specifies which QoS policy group to apply to the lun. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects

---

with which the policy group is associated. If you do not assign a policy group to a lun, the system will not monitor and control the traffic to it. To remove this lun from a policy group, enter the reserved keyword "none".

## Examples

```
cluster1::> lun modify -path /vol/vol1/lun1 -space-reserve disable
```

Disables the space reserve attribute for LUN /vol/vol1/lun1.

```
cluster1::> lun modify -path /vol/vol1/lun1 -state offline
```

Takes the LUN /vol/vol1/lun1 offline.

```
cluster1::> lun modify -path /vol/vol1/lun1 -comment "new comment"
```

Adds the comment "new comment" to the LUN /vol/vol1/lun1.

---

## lun move

Move (rename) a LUN

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

### Description

This command moves a LUN to a new path in the same volume or renames a LUN. If you are organizing LUNs in a qtree, the command moves a LUN from one qtree to another. LUNs cannot be moved out of a volume.

You can perform a LUN move while the LUN is online and serving data. The process is non-disruptive.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the existing path of the LUN you want to move.

| **-volume** <volume name> - Volume Name

Specifies the existing volume of the LUN you want to move.

  [**-qtree** <text>] - Qtree Name

Specifies the existing qtree of the LUN you want to move.

**-lun** <text> } - LUN Name

Specifies the name of the LUN that you want to move.

{ **-new-path** <path> - New LUN Path

Specifies the new path of the LUN.

| [**-new-qtree** <text>] - New Qtree Name

---

Specifies the new qtree name that you want to move the LUN to.

**-new-lun <text> }** - New LUN Name

Specifies the new name of the LUN.

## Examples

```
cluster1::> lun move -vserver vs1 -volume vol1 -lun lun1 -new-lun newlun1
```

Renames lun1 to newlun1 on Vserver vs1 and volume vol1.

```
cluster1::> lun show -vserver vs1 -volume vol1
Vserver  Path                                     State  Mapped  Type      Size
-----  -
vs1      /vol/vol1/A/lun1                       online mapped  linux     10MB

cluster1::> lun move -vserver vs1 -path /vol/vol1/A/lun1 -new-path /vol/vol1/B/
lun1

cluster1::> lun show -vserver vs1 -volume vol1
Vserver  Path                                     State  Mapped  Type      Size
-----  -
vs1      /vol/vol1/B/lun1                       online mapped  linux     10MB
```

Moves LUN lun1 from qtree A to qtree B on volume vol1.

---

## lun resize

Changes the size of the LUN to the input value size.

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

### Description

This command resizes a LUN. You can resize a LUN that is mapped and online. However, to prevent any potential problems, take the LUN offline before resizing it.

When you reduce the size of the LUN, the data in the LUN could be truncated. You will receive an error message if you reduce the size of the LUN. To avoid this error message, use the *force* parameter.

When you increase the size of a LUN, the maximum resize size is based on the initial geometry of the LUN and the currently available space in the volume. You will receive an error message if you exceed this limit. The `lun show -instance` command reports the "Maximum Resize Size" for a LUN based on the initial geometry. The `lun maxsize` command reports the maximum LUN size based on the available space. The maximum size of the LUN is the smaller of the two limits issued by the `lun show -instance` command or the `lun maxsize` command.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the LUN that you want to resize.

| **-volume** <volume name> - Volume Name

Specifies the volume that contains the LUN that you want to resize.

**-qtree** <text>] - Qtree Name

Specifies the qtree that contains the LUN that you want to resize.

---

**-lun <text> }** - LUN Name

Specifies the LUN name that you want to resize.

**[-force | -f [true]]** - Force Reduce LUN Size

Overrides any warnings if you are reducing the size of the LUN. If you use this parameter without a value, it is set to true, and the command does not prompt you when reducing the size of a LUN would produce warnings. If you do not use this parameter, the command displays an error if reducing the size of a LUN would create a problem.

**[-size <size>]** - New Size

Specifies the new size of the LUN.

- c (1 byte)
- w (2 bytes)
- B (512 bytes)
- k (1024 bytes)
- M (k\*k bytes)
- G (k\*m bytes)
- T (m\*m bytes)

## Examples

```
cluster1::> lun resize -vserver vs1 -path /vol/vol1/lun1 -size 500M -force
```

Resizes LUN /vol/vol1/lun1 on Vserver vs1 to 500M, overriding all warnings.

```
cluster1::> lun resize -vserver vs1 -path /vol/vol1/lun1 -size +5m
```

```
cluster1::> lun show -vserver vs1 -volume vol1
Vserver  Path                State  Mapped  Type      Size
-----
vs1      /vol/vol1/lun1      online mapped   linux    15MB
```

Adds 5M of space to LUN /vol/vol1/lun1 for a total of 15MB.

```
cluster1::> lun resize -vserver vs1 -path /vol/vol1/lun1 -size -10m
```

```
Error: command failed: Reducing LUN size without coordination with the host
system
      may cause permanent data loss or corruption. Use the force flag to allow
      LUN size reduction.
```

```
cluster1::> lun resize -path /vol/vol1/lun1 -size -5m -f
```

```
cluster1::> lun show -vserver vs1 -volume vol1
Vserver  Path                State  Mapped  Type      Size
-----
vs1      /vol/vol1/lun1      online mapped   linux    10MB
```

---

Resizes the LUN /vol/vol1/lun1 from 15MB to 10MB, overriding all warnings.

## **See Also**

lun show   lun maxsize

---

## lun show

Display a list of LUNs

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

### Description

The command displays information for LUNs. Use the `instance` option to display additional LUN details, such as serial number and space-reservation settings.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver Name

Selects the LUNs that match this parameter value.

{ [-**path** <path>] - LUN Path

Selects the LUNs that match this parameter value.

| [-**volume** <volume name>] - Volume Name

Selects the LUNs that match this parameter value.

[-**qtree** <text>] - Qtree Name

Selects the LUNs that match this parameter value.

[-**lun** <text>] } - LUN Name

Selects the LUNs that match this parameter value.

[-**size** | -**s** <size>] - LUN Size

Selects the LUNs that match this parameter value.



---

**[-prefix-size | -P <size>]** - Prefix Size (privilege: advanced)

Selects the LUNs that match the prefix stream size that you specify.

**[-ostype | -t <os\_enum>]** - OS Type

Selects the LUNs that match this parameter value. The OS types are:

- `aix` - the LUN stores AIX data.
- `hpux` - the LUN stores HP-UX data.
- `hyper_v` - the LUN stores Windows Server 2008 or Windows Server 2012 Hyper-V data
- `linux` - the LUN stores a Linux raw disk without a partition table.
- `netware` - the LUN stores NetWare data.
- `openvms` - the LUN store Open-VMS data
- `solaris` - the LUN stores Solaris raw disk in a single-slice partition.
- `solaris_efi` - the LUN stores Solaris\_EFI data.
- `vmware` - the LUN stores VMware data
- `windows` - the LUN stores a raw disk type in a single-partition Windows disk using the Master Boot Record (MBR) partitioning style.
- `windows_gpt` - the LUN stores Windows data using the GUID Partition Type (GPT) partitioning style.
- `windows_2008` - the LUN stores Windows data for Windows 2008 and 2012 systems.
- `xen` - the LUN stores Xen data

**[-space-reserve {enabled|disabled}]** - Space Reservation

Selects the LUNs that match this parameter value. If `true`, the LUN is space-reserved. If `false`, the LUN is thinly provisioned. The default is `true`.

**[-serial <text>]** - Serial Number

Selects the LUNs that match this parameter value.

**[-comment <text>]** - Comment

Selects the LUNs that match this parameter value.

**[-space-reserve-honored {true|false}]** - Space Reservations Honored

---

Selects the LUNs that match this parameter value. A value of `true` displays the LUNs that have space reservation honored by the container volume. A value of `false` displays the LUNs that are thinly provisioned.

**[-space-allocation {enabled|disabled}]** - Space Allocation

Selects the LUNs that match this parameter value. If you set this parameter to `enabled`, space allocation is enabled and provisioning threshold events for the LUN are reported. If you set this parameter to `disabled`, space allocation is not enabled and provisioning threshold events for the LUN are not reported.

**[-state <lunState\_enum>]** - State

Selects the LUNs that match this parameter value. The states are:

- `online`
- `offline`

**[-uuid <UUID>]** - LUN UUID

Selects the LUNs that match this parameter value.

**[-mapped {mapped|unmapped}]** - Mapped

Selects the LUNs that match this parameter value. A value of `mapped` selects the LUNs that are mapped to an initiator group.

**[-block-size <size>]** - Block Size

Selects the LUNs that match this parameter value.

**[-device-legacy-id <integer>]** - Device Legacy ID

Selects the LUNs that match this parameter value.

**[-device-binary-id <text>]** - Device Binary ID

Selects the LUNs that match this parameter value.

**[-device-text-id <text>]** - Device Text ID

Selects the LUNs that match this parameter value.

**[-read-only {true|false}]** - Read Only

Selects the LUNs that match this parameter value.

**[-restore-inaccessible {true|false}]** - Inaccessible Due to Restore

Selects the LUNs that match the state you specify. A value of `true` means that a LUN is inaccessible for I/O and management due to a restore operation.

---

**[-size-used <size>]** - Used Size

Selects the LUNs that match this parameter value.

**[-max-resize-size <size>]** - Maximum Resize Size

Selects the LUNs that match this parameter value.

**[-creation-timestamp <MM/DD/YYYY HH:MM:SS>]** - Creation Time

Selects the LUNs that match this parameter value.

**[-class {regular|protocol-endpoint|vvol}]** - Class

Selects the LUNs that match this parameter value.

**[-is-clone {true|false}]** - Clone

Selects the LUNs that match this parameter value.

**[-is-clone-autodelete-enabled {true|false}]** - Clone Autodelete Enabled

Selects the LUNs that match this parameter value.

**[-qos-policy-group <text>]** - QoS Policy Group

Selects the LUNs that match this parameter value.

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

## Examples

```
cluster1::> lun show -vserver vs0 -path /vol/vol1/lun1 -instance
      Vserver Name: vs0
      LUN Path: /vol/vol1/lun1
      Volume Name: vol1
      Qtree Name: ""
      LUN Name: lun1
      LUN Size: 10MB
      OS Type: linux
      Space Reservation: disable
      Serial Number: 1k/wc+9Cpb1s
      Comment: new comment
Space Reservations Honored: true
      Space Allocation: disable
      State: offline
      LUN UUID: 6435dcaa-e360-11df-aa84-00a0980cb0eb
      Mapped: unmapped
      Block Size: 512.00B
Device Legacy ID: -
Device Binary ID: -
Device Text ID: -
      Read Only: false
      Used Size: 0.00B
```

The example above displays details of the LUN at path /vol/vol1/lun1 in Vserver vs0.

```
cluster1::> lun show -serial 1r/wc+9Cpb1s
Vserver  Path                               State  Mapped  Type      Size
```

---

---

vs1	/vol/vol1/linux	offline mapped	linux	10MB
-----	-----------------	----------------	-------	------

The example above displays information for the LUN with serial number 1r/wc+9Cpbls.

```
cluster1::> lun show -vserver vs1 -volume vol1
Vserver  Path                               State  Mapped  Type      Size
-----  -
vs1      /vol/vol1/linux                   offline mapped  linux     10MB
vs1      /vol/vol1/windows                 online  mapped  windows   47.07MB
2 entries were displayed.
```

The example above displays all the LUNs on Vserver vs1 and volume vol1.

---

## lun unmap

Remove a previously configured LUN mapping.

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

### Description

This command unmaps a LUN from an initiator group. After you use this command, the LUN is not visible to any of the initiators in the initiator group.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the LUN you want to unmap.

| **-volume** <volume name> - Volume Name

Specifies the volume of the LUN you want to unmap.

**-qtree** <text>] - Qtree Name

Specifies the qtree of the LUN you want to unmap.

**-lun** <text> } - LUN Name

Specifies the name of the LUN you want to unmap.

**-igroup** <text> - Initiator Group Name

Specifies the initiator group that you want to unmap the LUN from.

### Examples

```
cluster1::> lun unmap -vserver vs1 -path /vol/vol1/lun1 -igroup ig1
```

Unmaps LUN at path /vol/vol1/lun1 from the initiator group ig1 on Vserver vs1.

---

## lun bind create

Bind a VVol LUN to a protocol endpoint

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

### Description

This command creates a new binding between a protocol endpoint and a vvol LUN. If a binding between the specified endpoint and vvol already exists, the reference count for the binding is incremented by one.

Note:

For optimal results, the protocol endpoint and vvol must be hosted by the same node in the cluster.

### Parameters

**-vserver** <vserver name> - Vserver name

Specifies the name of the Vserver.

**-protocol-endpoint-path** <path> - Protocol Endpoint

Specifies the path to the protocol endpoint. The specified LUN must already exist and be of class "protocol-endpoint".

**-vvol-path** <path> - VVol Path

Specifies the path to the vvol. The specified LUN must already exist and be of the class "vvol".

### Examples

```
cluster::*> lun bind create -vserver vs1 -protocol-endpoint-path /vol/VV1/PE1 -  
vvol-path /vol/VV3/234ace
```

Bind the vvol /vol/VV3/234ace to the protocol endpoint /vol/VV1/PE1 in Vserver vs1.

---

## lun bind destroy

Unbind a VVol LUN from a protocol endpoint

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

### Description

Decrement the reference count of the binding between a protocol endpoint and vvol LUN. If the resulting reference count is zero, the binding is removed.

### Parameters

**-vserver** <vserver name> - Vserver name

Specifies the Vserver.

**-protocol-endpoint-path** <path> - Protocol Endpoint

Specifies the path of the protocol endpoint LUN.

**-vvol-path** <path> - VVol Path

Specifies the path of the vvol LUN.

**[-force [true]]** - If true, unbind the Vvol completely even if the current reference count is greater than 1. The default is false.

Completely remove the specified binding, regardless of the current reference count.

### Examples

```
cluster::*> lun bind destroy -protocol-endpoint-path /vol/VV2/PE2 -vvol-path /  
vol/VV2/30dfab -vserver vs1
```

Remove the binding between the vvol /vol/VV2/30dfab and the protocol endpoint /vol/VV2/PE2 on Vserver vs1.

---

## lun bind show

Show list of Vvol bindings

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

### Description

Shows the configured VVol to protocol endpoint bindings.

### Parameters

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

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

| [-instance ] }

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

**[-vserver <vserver name>]** - Vserver

Selects the bindings that match this parameter value.

**[-protocol-endpoint-msid <integer>]** - PE MSID

Selects the bindings that match this parameter value.

**[-protocol-endpoint-vdisk-id <text>]** - PE Vdisk ID

Selects the bindings that match this parameter value.

**[-vvol-msid <integer>]** - VVol MSID

Selects the bindings that match this parameter value.

**[-vvol-vdisk-id <text>]** - VVol Vdisk ID

Selects the bindings that match this parameter value.

**[-vserver-uuid <UUID>]** - Vserver UUID

Selects the bindings that match this parameter value.

**[-protocol-endpoint-path <path>]** - Protocol Endpoint



---

Selects the bindings that match this parameter value.

**[-protocol-endpoint-node <nodename>]** - PE Node

Selects the bindings that match this parameter value.

**[-vvol-path <path>]** - VVol

Selects the bindings that match this parameter value.

**[-vvol-node <nodename>]** - VVol Node

Selects the bindings that match this parameter value.

**[-secondary-lun <Hex 64bit Integer>]** - Secondary LUN

Selects the bindings that match this parameter value.

**[-is-optimal {true|false}]** - Optimal binding

Selects the bindings that match this parameter value.

**[-vvol-uuid <UUID>]** - VVol UUID

Selects the bindings that match this parameter value.

**[-reference-count <integer>]** - Reference Count

Selects the bindings that match this parameter value.

## Examples

```
cluster::*> lun bind show -vserver vs1
Vserver      Protocol Endpoint      Node      Secondary LUN Optimal?
              Vvol  LUN
-----
vs1           /vol/VV1/PE1            cluster-node1
              /vol/VV2/30dfab         d20000010000 false
              /vol/VV3/234ace         d20000020000 true
              /vol/VV3/234acf         d20000030000 true
              /vol/VV2/PE2            cluster-node2
              /vol/VV2/30dfab         d20000010000 true
4 entries were displayed.
```

The example above displays all the LUN bindings on Vserver vs1.

---

## lun igroup add

Add initiators to an initiator group

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

### Description

This command adds initiators to an existing initiator group (igroup). You can add an initiator to an initiator group only if there are no LUN mapping conflicts. Mapping conflicts occur when an initiator is already paired with a LUN. If you attempt to run this command and there are LUN mapping conflicts, the command returns an error.

An initiator cannot be a member of two igroups of different OS types. For example, if you have an initiator that belongs to a Solaris igroup, the command does not allow you to add this initiator to an AIX igroup.

When you add FCP initiators, you can specify an alias instead of the initiator's World Wide Port Name (WWPN) or the iSCSI Qualified name (IQN).

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group to which you want to add a new initiator.

**-initiator** <text>, ... - Initiators

Specifies the initiator that you want to add. You can specify the WWPN, IQN, or alias of the initiator.

### Examples

```
cluster1::> lun igroup add -vserver vs1 -igroup ig1 -initiator  
iqn.1992-08.com.mv.mvinitiator
```

---

Adds the initiator `iqn.1992-08.com.mv.mvinitiator` to the initiator group `ig1` on Vserver `vs1`.

---

## lun igroup bind

Bind an existing initiator group to a given portset

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

### Description

This command binds an initiator group to a port set so the host knows which LIFs or TPGs to access. When you bind a port set to an igroup, the host knows which iSCSI or FCP LIF to access. If you do not bind an igroup to a port set, and you map a LUN to the igroup, then the initiators in the igroup can access the LUN on any port on the Vserver.

The initiator group cannot be bound to another port set when you use this command. If you attempt to bind a port set to an initiator group that is already bound to an existing port set, the command returns an error. You can only bind an initiator group to one port set at a time.

If the initiator group is bound, use the `lun igroup unbind` command to unbind the initiator group from the port set. After the initiator group is unbound, you can bind it to another port set.

You can only bind an initiator group to a non-empty port set.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group that you want to bind a port set to.

**-portset** <text> - Portset Binding Igroup

Specifies the port set name that you want to bind an initiator group to.

### Examples

```
cluster1::>lun igroup bind -vserver vs1 -igroup ig1 -portset-name ps1
```

---

Binds igroup ig1 to port set ps1.

## **See Also**

lun igroup unbind

---

## lun igroup create

Create a new initiator group

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

### Description

This command creates a new initiator group (igroup). Use igroups to control which hosts have access to specific LUNs. When you bind an igroup to a port set, a host in the igroup can access the LUNs only by connecting to the target ports in the port set.

When you create an igroup, you can add multiple existing initiators by specifying them in a list, separating them with commas. Later, you can add or remove initiators from the initiator group. Use the `lun igroup add` command to add initiators. Use the `lun igroup remove` command to remove an initiator.

You can also bind a port set to an initiator when you create an initiator group. You can modify the port set binding of an initiator group by using the `lun igroup bind` command or the `lun igroup unbind` command.

The name you assign to an igroup is independent of the name of the host that is used by the host operating system, host files, or Domain Name Service (DNS). If you name an igroup `aix1`, for example, it is not mapped to the actual IP host name (DNS name) of the host.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the name of the new initiator group. An initiator group name is a case-sensitive name and has the following requirements:

- Must contain one to 96 characters. Spaces are not allowed.

- 
- Can contain the letters A through Z, a through z, numbers 0 through 9, hyphen (-), underscore (\_), colon (:), and period (.).
  - Must start with a letter or number.

Note:

It might be useful to provide meaningful names for igroups, ones that describe the hosts that can access the LUNs mapped to them.

{ **[-protocol <protocol\_enum>]** - Protocol

Specifies if the initiator group protocol is FCP, iSCSI, or mixed.

| **[-fcp | -f [true]]** - FCP

If the initiator group protocol is FCP, set this parameter to true.

| **[-iscsi | -i [true]]** } - iSCSI

If the initiator group protocol is iSCSI, set this parameter to true.

**-ostype | -t <igroup\_os\_enum>** - OS Type

Specifies the operating system type for the new initiator group. The operating system type indicates the type of host operating system used by all of the initiators in the igroup. All initiators in an igroup must be of the same operating system type. The operating system types of initiators are

- solaris
- windows
- hpux
- aix
- linux
- netware
- vmware
- openvms
- xen
- hyper\_v

**[-portset | -a <text>]** - Portset Binding Igroup

Specifies that a port set is bound to the initiator.

---

**-initiator** <text>, ... - Initiators

Specifies the initiators that are attached to the new initiator group.

## Examples

```
cluster1::> lun igroup create -vserver vs1 -igroup ig1 -protocol-type mixed -  
ostype linux -initiator iqn.1992-08.com.mv.mvinitiator
```

Creates initiator group ig1 on Vserver vs1 with a mixed protocol type on a Linux operating system with the initiator iqn.1992-08.com.mv.mvinitiator.

## See Also

lun igroup add   lun igroup remove   lun igroup bind   lun igroup unbind



---

## lun igroup delete

Delete an initiator group

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

### Description

This command deletes an existing initiator group. By default, you cannot delete an initiator group if LUN maps for that initiator group exist. You need to unmap all the LUNs that are associated with that initiator group before you can delete the initiator group. Use the `lun unmap` command to remove LUNS from an initiator group.

You can specify the `force` option to delete an initiator group and remove existing LUN maps defined for that initiator group.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group that you want to delete.

**[-force | -f [true]]** - Force

Deletes an initiator group and all associated LUN maps.

### Examples

```
cluster1::>lun igroup delete -vserver vs1 -igroup ig1
```

Deletes the initiator group ig1 on Vserver vs1.

### See Also

`lun unmap`

---

## lun igroup disable-aix-support

Disables SAN AIX support on the cluster

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

### Description

This command disables the SAN AIX support across the cluster (all Vservers and all AIX initiator groups). However, before you can disable SAN AIX support, you must remove all SAN AIX related objects from the cluster. You need to unmap all the LUNs that are associated with the AIX initiator groups. Then you need to delete all of the AIX initiator groups. Use the `lun unmap` command to remove LUNS from an initiator group. Use the `igroup delete` command to delete an initiator group.

Note:

This command is not intended to be used in normal operation. Use only when you are downgrading to a release that does not support SAN AIX operation.

### Parameters

None

### Examples

```
cluster1::>lun igroup disable-aix-support
```

Disables the SAN AIX support for cluster1.

### See Also

`lun unmap` `igroup delete`

---

## lun igroup modify

Modify an existing initiator group

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

### Description

This command modifies an attribute for an initiator group. For example, you can change the operating system setting.

When you create a new initiator group, the ALUA setting is enabled by default.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group whose attribute you want to modify.

**[-ostype | -t** <igroup\_os\_enum>] - OS Type

Specifies the operating system that you want to modify. The operating system types of initiators are

- solaris
- windows
- hpux
- aix
- linux
- netware
- vmware
- openvms

- 
- xen
  - hyper\_v

## Examples

```
cluster1::>lun igroup modify -vserver vs1 -igroup ig1 -ostype windows
```

Changes the operating system to windows for initiator group ig1 on Vserver vs1.

---

## lun igroup remove

Remove initiators from an initiator group

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

### Description

This command removes an initiator from an initiator group. You can only remove an initiator if no existing LUN maps are defined for that initiator group. You must unmap the LUNs from the initiator group with the `lun unmap` command before you can remove initiators from the initiator group.

You can use the *force* option to remove an initiator and associated LUN maps.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group from which you want to remove an initiator.

**-initiator** <text>, ... - Initiators

Specifies the initiator name you want to remove. Use the WWPN, IQN or the alias of the initiator.

**[-force | -f [true]]** - Force

Forcibly removes an initiator and any associated LUN maps.

### Examples

```
cluster1::> lun igroup remove -vserver vs1 -igroup ig1 -initiator  
iqn.1992-08.com.mv.mvinitiator
```

Removes the initiator `iqn.1992-08.com.mv.mvinitiator` from Vserver `vs1` and initiator group `ig1`.

---

## See Also

`lun unmap`

---

## lun igroup rename

Rename an existing initiator group

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

### Description

This command renames an existing initiator group. When you rename an initiator group, this action does not affect access to the LUNs mapped to the initiator group you want to rename.

An initiator group name is a case-sensitive name and must meet the following requirements:

- Must contain one to 96 characters. Spaces are not allowed.
- Can contain the letters A through Z, a through z, numbers 0 through 9, hyphen (-), underscore (\_), colon (:), and period (.).
- Must start with a letter or number.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group you want to rename.

**-new-name** <text> - New Igroup Name

Specifies the new name of the initiator group.

### Examples

```
cluster1::> lun igroup rename -vserver vs1 -igroup ig1 -new-name ignew1
```

Renames an initiator group from ig1 to ignew1 on Vserver vs1.

---

## lun igroup show

Display a list of initiator groups

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

### Description

This command displays status information for initiator groups (igroup). By default, the command displays status for all initiator groups.

### Parameters

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

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

| [-instance ] }

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

**[-vserver <vserver name>]** - Vserver Name

Specifies the Vserver.

**[-igroup <text>]** - Igroup Name

Selects the initiator groups that match this parameter value.

**[-protocol <protocol\_enum>]** - Protocol

Selects the initiator groups that match this parameter value (FCP, iSCSI, or mixed).

**[-ostype | -t <igroup\_os\_enum>]** - OS Type

Selects the initiator groups that match this parameter value. The operating system types are

- solaris
- windows
- hpux
- aix



- 
- linux
  - netware
  - vmware
  - openvms
  - xen
  - hyper\_v

**[-portset | -a <text>] - Portset Binding Igroup**

Selects the initiator groups that match this parameter value.

**[-initiator <text>, ...] - Initiators**

Selects the initiator groups that match this parameter value.

**[-uuid <UUID>] - Igroup UUID**

Selects the initiator groups that match this parameter value.

## Examples

```
cluster1::> igroup show -instance
      Vserver Name: vs0
      Igroup Name: ig1
      Protocol: mixed
      OS Type: linux
Portset Binding Igroup: -
      Igroup UUID: 358338ba-cfd6-11df-a9ab-123478563412
      Initiators: iqn.1992-08.com.mv:abc (not logged in)

      Vserver Name: vs0
      Igroup Name: ig2
      Protocol: mixed
      OS Type: linux
Portset Binding Igroup: -
      Igroup UUID: 3fb136c7-cfd6-11df-a9ab-123478563412
      Initiators: -

      Vserver Name: vs1
      Igroup Name: ig1
      Protocol: mixed
      OS Type: windows
Portset Binding Igroup: pl
      Igroup UUID: 03accf6b-d08c-11df-a9ab-123478563412
      Initiators: -
3 entries were displayed.
```

The example above displays information about all initiator groups in node1.

---

## lun igroup unbind

Unbind an existing initiator group from a portset

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

### Description

This command unbinds an initiator group from a port set. When you unbind an initiator group from a port set, all of the initiators in the initiator group have access to all target LUNs on all network interfaces.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-igroup** <text> - Igroup Name

Specifies the initiator group that you want to unbind from the port set.

### Examples

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

Unbinds the initiator group ig1 from the port set on Vserver vs1.

---

## lun mapped show

Lists the mappings between LUNs and initiator groups.

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

### Description

This command lists the mappings between LUNs and initiator groups.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver Name

Selects the LUN maps for the Vserver that matches the parameter value.

{ [-**path** <path>] - LUN Path

Selects the LUN maps for the LUN with the path that matches the parameter value.

| [-**volume** <volume name>] - Volume Name

Selects the LUN maps for the volumes that match the parameter value.

[-**qtree** <text>] - Qtree Name

Selects the LUN maps for the queue trees that match the parameter value.

[-**lun** <text>] } - LUN Name

Selects the LUN maps for the LUNs with a name that matches the parameter value.

[-**igroup** | -**g** <text>] - Igroup Name

Selects the LUN maps for the igroup that matches the parameter value.

[-**ostype** <igroup\_os\_enum>] - Igroup OS type

Selects the LUN maps for the initiator groups with the OS type that matches the parameter value. The possible OS types are:

- `solaris` - the LUN stores Solaris raw disk in a single-slice partition.
- `windows` - the LUN stores a raw disk type in a single-partition Windows disk using the Master Boot Record (MBR) partitioning style.
- `hpux` - the LUN stores HP-UX data.
- `linux` - the LUN stores a Linux raw disk without a partition table.
- `netware` - the LUN stores NetWare data.
- `vmware` - the LUN stores VMware data
- `openvms` - the LUN store Open-VMS data
- `xen` - the LUN stores Xen data
- `hyper_v` - the LUN stores Hyper-V data

**[-protocol <protocol\_enum>]** - Igroup Protocol Type

Selects the LUN maps for initiator groups with a protocol that matches the parameter value. Possible values include FCP, iSCSI, or mixed.

**[-lun-id <integer>]** - LUN ID

Selects the LUN maps with a LUN ID that matches the parameter value.

**[-portset <text>]** - Portset Binding Igroup

Selects the LUN maps for initiator groups bound to the portset that matches the parameter value.

**[-alua {true|false}]** - ALUA

Selects the LUN maps with ALUA settings that match the parameter value.

**[-initiators | -n <text>, ...]** - Initiators

Selects the LUN maps for initiator groups containing the initiators that match the parameter value.

## Examples

```
cluster1::> lun mapped show
Vserver      Path
-----
vs1          /vol/vol1/lun1
vs1          /vol/vol1/lun1
vs1          /vol/vol5/lun1
vs1          /vol/vol5/lun2
4 entries were displayed.
```

Igroup	LUN ID	Protocol
igroup1	10	mixed
igroup2	4	mixed
igroup3	6	mixed
igroup3	1	mixed

---

The example above lists all of the mappings between LUNs and initiator groups and the LUN ID for each mapping.

---

## lun persistent-reservation clear

Clear the SCSI-3 persistent reservation information for a given LUN

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

### Description

Clears the persistent reservation for the specified LUN.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-path** <path> - LUN Path

Specifies the path of the LUN.

| **-volume** <volume name> - Volume Name

Specifies the volume.

**[-qtree <text>]** - Qtree Name

Specifies the qtree.

**-lun <text> }** - LUN Name

Specifies the name of the LUN.

### Examples

```
cluster1::*> lun persistent-reservation clear -vserver vs_1 -path /vol/vol_1/  
lun_1
```

Clears the persistent reservation data for lun lun\_1 in volume vol\_1 for Vserver vs\_1.

---

## lun persistent-reservation show

Display the current reservation information for a given LUN

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

### Description

Displays reservation information for a specified LUN in a Vserver. Unlike other show commands, the user must specify the LUN.

### Parameters

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

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

| [-**instance**] }

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

[-**vserver** <vserver name>] - Vserver Name

Specifies the Vserver.

{ [-**path** <path>] - LUN Path

Specifies the path of the LUN.

| [-**volume** <volume name>] - Volume Name

Specifies the volume.

[-**qtree** <text>] - Qtree Name

Specifies the qtree.

[-**lun** <text>] } - LUN Name

Specifies the name of the LUN.

[-**scsi-revision** {scsi2|scsi3}] - SCSI Revision

Selects the reservations that match this parameter value.

---

**[-entry-type {reservation|registration}]** - Reservation or Registration

Selects the reservations that match this parameter value.

**[-protocol {fcpl|iscsi}]** - Protocol

Selects the reservations that match this parameter value.

**[-reservation-key <text>]** - Reservation Key

Selects the reservations that match this parameter value.

**[-reservation-type-code <text>]** - Reservation Type

Selects the reservations that match this parameter value. The possible values for SCSI-3 reservations are:

- write exclusive
- exclusive access
- write exclusive registrants only
- exclusive access registrants only
- write exclusive all registrants
- exclusive access all registrants

and for SCSI-2 are:

- regular
- third party

**[-initiator-name <text>]** - Initiator Name

Selects the reservations that match this parameter value.

**[-aptpl {true|false}]** - Persist Through Power Loss

Selects the reservations that match this parameter value. If `true`, the reservation will be preserved over a power loss. If `false`, it will not. This value is for SCSI-3 reservations only.

**[-target-wwpn <text>]** - FCP Target WWPN

Selects the reservations that match the specified World Wide Port Name (WWPN).

**[-isid <text>]** - Initiator Session ID

Selects the reservations that match this parameter value.

**[-tpgroup-tag <integer>]** - TPGroup Tag



---

Selects the reservations that match the specified target portal group tag. The tag identifies the tpgroup the reservation was made over.

**[-third-party-initiator-name <text>]** - Third Party Initiator Name

Selects the reservations that match this parameter value (the initiator name that the reservation was made for). This is specific to third party reservation types, which is indicated by reservation-type-code.

**Examples**

```
cluster1::*> lun persistent-reservation show -vserver vs_1 /vol/vol_1/lun_1
Key                                     Protocol Type                           Initiator Name
-----
APTPL: true
a0:00:00:00:00:00:00:01 iscsi           write exclusive
iqn.1993-08.org.debian:01:fa752b8a5a3a
a0:00:00:00:00:00:00:01 iscsi           -
iqn.1993-08.org.debian:01:fa752b8a5a3a
2 entries were displayed.
```

The example above displays the current reservations for lun\_1 on Vsever vs\_1.

---

## lun portset add

Add iSCSI/FCP LIFs to a portset

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

### Description

This command adds existing iSCSI and FCP LIFs to a port set. To create a new port set, use the `lun portset create` command.

Use the `network interface create` command to create new LIFs.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-portset** <text> - Portset Name

Specifies the port set you want to add the LIFs to.

**-port-name** <port\_name>, ... - LIF Name

Specifies the LIF name you want to add to the port set.

### Examples

```
cluster1::> portset add -vserver vs1 -portset ps1 -port-name lif1
```

Adds port lif1 to port set ps1 on Vserver vs1.

### See Also

`lun portset create`   `network interface create`

---

## lun portset create

Creates a new portset

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

### Description

This command creates a new port set for FCP and iSCSI. The port set name can include a maximum of 95 characters. You can add LIFs to the new port set. If you do not add a LIF to the port set, you create an empty port set. To add LIFs to an existing port set, use the `lun portset add` command.

After you create a port set, you must bind the port set to an igroup so the host knows which FC or iSCSI LIFs to access. If you do not bind an igroup to a port set, and you map a LUN to an igroup, then the initiators in the igroup can access the LUN on any LIF on the Vserver.

Note:

You cannot bind an igroup to an empty port set because the initiators in the igroup would have no LIFs to access the LUN.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-portset** <text> - Portset Name

Specifies the name of the port set. You can specify a string up to 95 characters.

**[-port-name** <port\_name>, ...] - LIF Name

Specifies the name of the logical interface that you want to add to the portset you want to create.

{ **[-protocol** <protocol\_enum>] - Protocol

---

Specifies if the portset protocol type is FCP, iSCSI, or mixed. The default is mixed.

| [-fcp | -f [true]] - FCP

Specifies FCP protocol of the new port set.

| [-iscsi | -i [true]] } - iSCSI

Specifies the iSCSI protocol of the new port set.

## Examples

```
cluster1::> portset create -vserver vs1 -portset ps1 -protocol mixed
```

Creates a port set ps1 on Vserver vs1 with the protocol type of mixed.

```
cluster1::> portset create -vserver vs1 -portset iscsips -protocol iscsi
```

Creates a port set iscsips on Vserver vs1 with the protocol type of iSCSI.

```
cluster1::> portset create -vserver vs1 -portset fcppc -protocol fcp
```

Creates a port set fcppc on Vserver vs1 with the protocol type of FCP.

```
cluster1::> portset create -vserver vs1 -portset ps2 -protocol mixed -port-name  
l11
```

Creates a port set ps2 on Vserver vs1 with the protocol type of mixed and LIF l11.

## See Also

lun portset add

---

## lun portset delete

Delete the portset

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

### Description

This command deletes an existing port set. By default, you cannot delete a port set if it is bound to an initiator group. If a port set is bound to an initiator group, you can do one of the following:

- specify the `force` option to unbind the port set from the initiator group and delete the port set.
- use the `lun igroup unbind` command to unbind the port set from the initiator group. Then you can delete the port set.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-portset** <text> - Portset Name

Specifies the port set you want to delete.

**[-force | -f [true]]** - Force

Forcibly unbinds the port set from the initiator group.

### Examples

```
cluster1::> portset delete -vserver vs1 -portset ps1
```

Deletes port set ps1 on Vserver vs1.

### See Also

---

lun igroup unbind

---

## lun portset remove

Remove iSCSI/FCP LIFs from a portset

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

### Description

This command removes a LIF from a port set.

You cannot remove the last LIF in a port set if the port set is bound to an initiator group (igroup). To remove the last LIF in a port set, use the `lun igroup unbind` command to unbind the port set from the igroup. Then you can remove the last LIF in the port set.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-portset** <text> - Portset Name

Specifies the port set you want to remove a LIF from.

**-port-name** <port\_name>, ... - LIF Name

Specifies the LIF name you want to remove from the port set.

### Examples

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Removes port lif1 from port set ps1 on Vserver vs1.

### See Also

`lun igroup unbind`

---

## lun portset show

Displays a list of portsets

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

### Description

This command displays the LIFs in a port set. By default, the command displays all LIFs in all port sets.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver Name

Specifies the Vserver.

[-**portset** <text>] - Portset Name

Selects the port sets that match this parameter value.

[-**port-name** <port\_name>, ...] - LIF Name

Selects the port sets that match this parameter value.

[-**protocol** <protocol\_enum>] - Protocol

Selects the port sets that match this parameter value.

[-**port-count** <integer>] - Number Of Ports

Selects the port sets that match this parameter value.

[-**igroups** <igroup>, ...] - Bound To Igroups

Selects the port sets that match this parameter value.



---

## Examples

```
cluster1:> portset show
(lun portset show)
```

Virtual Server	Portset	Protocol	Port Names	Igroups
js11	ps0	mixed	LIF1, LIF2	igroup1
	ps1	iscsi	LIF3	igroup2
	ps2	fcp	LIF4	igroup2

3 entries were displayed.

The example above displays the port sets and names on Vserver js11.

```
cluster1::> portset show -port-count 0
Vserver Portset Protocol Port Names Igroups
-----
```

vs1	p1	iscsi	-	-
-----	----	-------	---	---

The example above displays the port set p1 that contains zero LIFs on Vserver vs1.

```
cluster1::> portset show -protocol iscsi
Vserver Portset Protocol Port Names Igroups
-----
```

vs1	p1	iscsi	-	-
vs1	iscsips	iscsi	l11	igl

2 entries were displayed.

The example above displays port sets p1 and iscips that have iSCSI protocol on Vserver vs1.

```
cluster1::> portset show -port-name l11
Vserver Portset Protocol Port Names Igroups
-----
```

vs1	iscsips	iscsi	lif11	igl
-----	---------	-------	-------	-----

The example above displays port set information for LIF lif11 on Vserver vs1.

---

## network ping

Ping

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

### Description

The `network ping` command displays whether a remote address is reachable and responsive, the (if specified) number of transmitted and received packets, and their round-trip time. The command requires a source node or interface group from where the ping will be run, and a destination IP address. You can specify the source node by name, or an interface group and its Vserver.

### Parameters

{ **-node** <nodename> - Node

Use this parameter to send the ping from the node you specify.

| **-lif-owner** <vserver> - LIF Owner

Use this parameter to send the ping from the node where the interface group you specify resides.

**-lif** <lif-name> - Logical Interface

Use this parameter to send the ping from the interface group you specify.

**[-use-source-port {true|false}]** } - Use Source Port of Logical Interface (privilege: advanced)

This parameter is only applicable when the `-lif` parameter is specified. When set to true, the ping packet will be sent out via the port which is currently hosting the IP address of the logical interface. Otherwise, the ping packet will be sent out via a port based on the routing table.

**-destination** <Remote InetAddress> - Destination

Use this parameter to specify the remote internet address destination of the ping.

**[-show-detail | -s [true]]** - Show Detail Output

Use this parameter to display detailed output about the ping.

**[-record-route | -R [true]]** - Record Route

---

Use this parameter to display the route followed by the ping. You should set this option to `false` for ping to succeed.

**[-verbose | -v [true]]** - Show All ICMP Packets

Use this parameter to display all ICMP packets.

**[-packet-size <integer>]** - Packet Size

Use this parameter to specify the number of data bytes to be sent in the ping packet. The default is 56 bytes, which is 64 ICMP data bytes total after 8 bytes of ICMP header data is added.

**[-count <integer>]** - Count

Use this parameter to specify the number of ECHO\_REQUESTS to be sent to the destination. The default is 20 requests.

**[-wait <integer>]** - Wait between Packets (secs)

Use this parameter to specify the number of seconds to wait between sending packets. The default is one second.

**[-flood [true]]** - Flood Ping (privilege: advanced)

Use this parameter to execute the command in flood mode. In flood mode, the command issues pings as fast as they are received, unless you specify a wait time.

**[-disallow-fragmentation | -D [true]]** - Disallow Packet Fragmentation

Use this parameter to prevent transport mechanisms from fragmenting ping packets in transit. Preventing fragmentation assures consistent packet size, making it easier to see transport bottlenecks.

## Examples

This example shows a ping from node xena to the destination server 10.98.16.164 with the server responding that it is up and running.

```
cluster1::> ping -node xena -destination 10.98.16.164
(network ping)
10.98.16.164 is alive
```

## network traceroute

Traceroute

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

---

## Description

The `network traceroute` command performs a network probe from a node to a specified IP address. The command requires a source node or interface group and a destination IP address. You can specify the source node by name, or specify an interface group and its Vserver. The traceroute is performed between the source and destination.

## Parameters

{ **-node** <nodename> - Node

Use this parameter to originate the traceroute from the node you specify.

| **-lif-owner** <vserver> - LIF Owner

Use this parameter to originate the traceroute from the node where the interface group with the logical interface you specify resides.

**-lif** <lif-name> } - Logical Interface

Use this parameter to originate the traceroute from the interface group you specify.

**-destination** <Remote InetAddress> - Destination

Use this parameter to specify the remote internet address destination of the traceroute.

[**-maxttl** | **-m** <integer>] - Maximum Number of Hops

Use this parameter to specify the maximum number of hops (time-to-live) setting used by outgoing probe packets. The default is 30 hops.

[**-numeric** | **-n** [true]] - Print Hop Numerically

Use this parameter to print the hop addresses only numerically rather than symbolically and numerically.

[**-port** <integer>] - Base UDP Port Number

Use this parameter to specify the base UDP port number used in probes. The default is port 33434.

[**-packet-size** <integer>] - Packet Size

Use this parameter to specify the size of probe packets, in bytes.

[**-nqueries** | **-q** <integer>] - Number of Queries

Use this parameter to specify the number of probes per hop. The default is 3 probes.

[**-verbose** | **-v** [true]] - Verbose Output

---

Use this parameter to display all received ICMP packets, rather than just TIME\_EXCEEDED and UNREACHABLE packets.

**[-waittime | -w <integer>]** - Wait Between Packets (secs)

Use this parameter to specify the time (in seconds) to wait for the response to a probe. The default is 5 seconds.

## Examples

This example shows a traceroute from node node1 to a Vserver with a destination address of 10.98.16.164, showing a maximum of five hops.

```
cluster1::> traceroute -node node1 -destination 10.98.16.164 -maxttl 5
1  10.68.208.1 <10.68.208.1> 0.307 ms 293 ms 305 ms
2  152.164.13.205 <152.164.13.205> 3.754 ms 3.722 ms 3.981 ms
3  68.137.122.222 <68.137.122.222> 25.603 ms 24.947 ms 24,565 ms
4  * * *
5  * * *
```

traceroute to 10.98.16.164, 5 hops max, 52 byte packets

---

## network connections active show-clients

Show a count of the active connections by client

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

### Description

The `network connections active show-clients` command displays information about client connections, including the client's IP address and the number of client connections.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Use this parameter to display information only about the connections on the node you specify.

[-**remote-address** <Remote IP>] - Remote IP Address

Use this parameter to display information only about the connections that use the remote IP address you specify.

[-**count** <integer>] - Client Count

Use this parameter to only clients with the number of active client connections you specify.

### Examples

The following example displays information about active client connections:

```
cluster1::> network connections active show-clients
Node      Client IP Address      Count
-----
node0     192.0.2.253             1
```

---

	192.0.2.252	2
	192.0.2.251	5
node1	192.0.2.250	1
	192.0.2.252	3
	192.0.2.253	4
node2	customer.example.com	1
	192.0.2.245	3
	192.0.2.247	4
node3	192.0.2.248	1
	customer.example.net	3
	customer.example.org	4

---

## network connections active show-lifs

Show a count of the active connections by logical interface

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

### Description

The `network connections active show-lifs` command displays the number of active connections on each logical interface, organized by node and Vserver.

### Parameters

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

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

| [-instance ] }

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

**[-node {<nodename>|local}]** - Node

Use this parameter to display information only about the connections on the node you specify.

**[-vserver <vserver>]** - Vserver

Use this parameter to display information only about the connections that are using the node or Vserver you specify.

**[-lif-name <lif-name>]** - Logical Interface Name

Use this parameter to display information only about the connections that are using the logical interface you specify.

**[-count <integer>]** - Client Count

Use this parameter to display only logical interfaces with the number of active client connections you specify.

**[-blocked-count <integer>]** - Load Balancing Blocking Count



Use this parameter to display information only about data logical interfaces blocked from migrating and the connection that is blocking it.

### Examples

The following example displays information about the servers and logical interfaces being used by all active connections:

```
cluster1::> network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    vs0        cluslif1        6
    vs0        cluslif2        5
node1
    vs0        datalif2        3
    vs0        cluslif1        3
    vs0        cluslif2        5
node2
    vs1        datalif2        1
    vs1        cluslif1        5
    vs1        cluslif2        3
node3
    vs1        datalif1        1
    vs1        cluslif1        2
    vs1        cluslif2        1
```

At privilege levels above "admin", the command displays an extra column.

```
cluster1::*> network connections active show-lifs
Node      Vserver Name  Interface Name  Count  LB Migrate
-----
node0
    vs0        datalif1        3        0
    vs0        cluslif1        6        0
    vs0        cluslif2        5        2
node1
    vs0        datalif2        3        0
    vs0        cluslif1        3        0
    vs0        cluslif2        5        0
node2
    vs1        datalif2        1        0
    vs1        cluslif1        5        0
    vs1        cluslif2        3        2
node3
    vs1        datalif1        1        0
    vs1        cluslif1        2        0
    vs1        cluslif2        1        0
```

---

## network connections active show-protocols

Show a count of the active connections by protocol

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

### Description

The `network connections active show-protocols` command displays the number of active connections per protocol, organized by node.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Use this parameter to display information only about the connections on the node you specify.

[-**proto** {UDP|TCP}] - Protocol

Use this parameter to display information only about the connections that use the network protocol you specify. Possible values include `tcp` (TCP), `udp` (UDP), and `NA` (not applicable).

[-**count** <integer>] - Client Count

Use this parameter to display only protocols with the number of active client connections you specify.

### Examples

The following example displays information about all network protocols being used by active connections:

```
cluster1::> network connections active show-protocols
Node      Protocol      Count
-----
-----
```

---

node0	UDP	19
	TCP	11
node1	UDP	17
	TCP	8
node2	UDP	14
	TCP	10
node3	UDP	18
	TCP	4

---

## network connections active show-services

Show a count of the active connections by service

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

### Description

The `network connections active show-services` command displays the number of active connections by protocol service, organized by node.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Use this parameter to display information only about the connections on the node you specify.

[-service <protocol service>] - Protocol Service

Use this parameter to display information only about the connections that use the protocol service you specify. Possible values include: `nfs`, `iscsi`, and `loopback`.

[-count <integer>] - Client Count

Use this parameter to display information only about protocol services with the number of active client connections you specify.

### Examples

The following example displays information about all protocol services being used by active connections:

```
cluster1::> network connections active show-services
Node      Service      Count
-----
node0
```

---

	mount	3
	nfs	14
	nlm_v4	4
	cifs_srv	3
	port_map	18
	rclopcp	27
node1		
	cifs_srv	3
	rclopcp	16
node2		
	rclopcp	13
node3		
	cifs_srv	1
	rclopcp	17

---

## network connections active show

Show the active connections in this cluster

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

### Description

The `network connections active show` command displays information about active network connections.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the connections that match this parameter value.

[-**cid** <Cid>] - Connection ID

Selects the connections that match this parameter value.

[-**vserver** <vserver>] - Vserver

Selects the connections that match this parameter value.

[-**lif-name** <lif-name>] - Logical Interface Name

Selects the connections that match this parameter value.

[-**local-address** <IP Address>] - Local IP address

Selects the connections that match this parameter value.

[-**local-port** <integer>] - Local Port

Selects the connections that match this parameter value.

---

**[-remote-ip <InetAddress>]** - Remote IP Address

Selects the connections that match this parameter value.

**[-remote-host <Remote IP>]** - Remote Host

Selects the connections that match this parameter value.

**[-remote-port <integer>]** - Remote Port

Selects the connections that match this parameter value.

**[-proto {UDP|TCP}]** - Protocol

Selects the connections that match this parameter value. Possible values are tcp (TCP), udp (UDP), and NA (not applicable).

**[-lifid <integer>]** - Logical Interface ID

Selects the connections that match this parameter value.

**[-service <protocol service>]** - Protocol Service

Selects the connections that match this parameter value. Possible values include: nfs, iscsi, and loopback.

**[-lru {yes|no}]** - Least Recently Used

Selects the connections that match this parameter value.

**[-blocks-lb {true|false}]** - Connection Blocks Load Balance Migrate

Selects the logical interfaces that are blocked (true) or not blocked (false) from migrating due to an active client connection.

## Examples

The following example displays information about active network connections for the node named node0:

```
cluster1::> network connections active show node -node0
```

Vserver Name	Interface Name:Local Port	Remote IP Address:Port	Protocol/Service
node0	cluslif1:7070	192.0.2.253:48621	UDP/rclopcp
node0	cluslif1:7070	192.0.2.253:48622	UDP/rclopcp
node0	cluslif2:7070	192.0.2.252:48644	UDP/rclopcp
node0	cluslif2:7070	192.0.2.250:48646	UDP/rclopcp
node0	cluslif1:7070	192.0.2.245:48621	UDP/rclopcp
node0	cluslif1:7070	192.0.2.245:48622	UDP/rclopcp
node0	cluslif2:7070	192.0.2.251:48644	UDP/rclopcp
node0	cluslif2:7070	192.0.2.251:48646	UDP/rclopcp
node0	cluslif1:7070	192.0.2.248:48621	UDP/rclopcp
node0	cluslif1:7070	192.0.2.246:48622	UDP/rclopcp
node0	cluslif2:7070	192.0.2.252:48644	UDP/rclopcp
node0	cluslif2:7070	192.0.2.250:48646	UDP/rclopcp
node0	cluslif1:7070	192.0.2.254:48621	UDP/rclopcp
node0	cluslif1:7070	192.0.2.253:48622	UDP/rclopcp
[...]			

---

At privilege levels above "admin", the command displays an extra column.

```
cluster1::*> network connections active show node -node0
```

Vserver Name	Interface Name:Local Port	Remote IP Address:Port	Protocol/Service	Blocks LB Migrate
node0	cluslif1:7070	192.0.2.253:48621	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.253:48622	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.252:48644	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.250:48646	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.245:48621	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.245:48622	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.251:48644	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.251:48646	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.248:48621	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.246:48622	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.252:48644	UDP/rclopcp	false
node0	cluslif2:7070	192.0.2.250:48646	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.254:48621	UDP/rclopcp	false
node0	cluslif1:7070	192.0.2.253:48622	UDP/rclopcp	false

[...]



---

## network connections listening show

Show the listening connections in this cluster

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

### Description

The `network connections listening show` command displays information about network connections that are in an open and listening state.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the listening connections that match this parameter value.

[-**mgmt-cid** <integer>] - Management Connection ID

Selects the listening connections that match this parameter value.

[-**vserver** <vserver>] - Vserver

Selects the listening connections that match this parameter value.

[-**cid** <integer>] - System Connection ID

Selects the listening connections that match this parameter value.

[-**lif-name** <lif-name>] - Logical Interface Name

Selects the listening connections that match this parameter value.

[-**local-address** <IP Address>] - Local IP Address

Selects the listening connections that match this parameter value.

---

**[-local-port <integer>]** - Local Port

Selects the listening connections that match this parameter value.

**[-remote-ip <InetAddress>]** - Remote IP Address

Selects the listening connections that match this parameter value.

**[-remote-host <Remote IP>]** - Remote Host

Selects the listening connections that match this parameter value.

**[-remote-port <integer>]** - Remote Port

Selects the listening connections that match this parameter value.

**[-proto {UDP|TCP}]** - Protocol

Selects the listening connections that match this parameter value. Possible values include tcp (TCP), udp (UDP), and NA (not applicable).

**[-lifid <integer>]** - Logical Interface ID

Selects the listening connections that match this parameter value.

**[-service <protocol service>]** - Protocol Service

Selects the listening connections that match this parameter value. Possible values include: nfs, iscsi, and loopback.

**[-lru {yes|no}]** - Least Recently Used

Selects the listening connections that match this parameter value.

## Examples

The following example displays information about all listening network connections:

```
cluster1::> network connections listening show
Vserver Name Interface Name:Local Port Protocol/Service
-----
node0        cluslif1:7700 UDP/rclopcp
node0        cluslif2:7700 UDP/rclopcp
node1        cluslif1:7700 UDP/rclopcp
node1        cluslif2:7700 UDP/rclopcp
node2        cluslif1:7700 UDP/rclopcp
node2        cluslif2:7700 UDP/rclopcp
node3        cluslif1:7700 UDP/rclopcp
node3        cluslif2:7700 UDP/rclopcp
8 entries were displayed.
```

The following example displays detailed information about listening network connections for the node named node0:

```
cluster1::> network connections listening show -node node0
Node: node0
Management Connection Id: 0
System Connection Id: 0
Vserver: vs0
```

---

```
Logical Interface Name: datalif1
  Local IP address: 192.0.2.130
  Local Port: 111
  Remote IP address:
  Remote Port: 0
  Protocol: UDP
Logical Interface Id: 1029
  Protocol Service: port_map
  least recently used: yes
  Node: node0
Management Connection Id: 1
System Connection Id: 0
  Server: vs0
Logical Interface Name: datalif2
  Local IP address: 192.0.2.131
  Local Port: 111
  Remote IP address:
  Remote Port: 0
  Protocol: UDP
Logical Interface Id: 1030
  Protocol Service: port_map
  least recently used: yes
```

---

## network fcp adapter modify

Modify the fcp adapter settings

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

### Description

Modifies the FCP target adapter information.

The adapter argument is in the form Xy or Xy\_z where X and z are integers and y is a letter. An example is 4a or 4a\_1.

You cannot bring an adapter offline until all logical interfaces connected to that adapter are offline. Use the `network interface modify` command to take your logical interfaces offline.

The speed option sets the Fibre Channel link speed of an adapter. You can set adapters that support:

- 10Gb/s to 10 or auto
- 8Gb/s to 2, 4, 8 or auto
- 4Gb/s to 2, 4 or auto
- 2Gb/s to 2 or auto

By default, the link speed option is set to auto for auto negotiation. If you set the link speed to a specific value, this change disables the auto negotiation. Under certain conditions, a speed mismatch can prevent the adapter from coming online.

Note:

The system reports the actual link speed with the "Link Data Rate" parameter in the output of `network fcp adapter show -instance`.

### Parameters

**-node** {<nodename>|local} - Node

Specifies the node of the target adapter.

**-adapter** <text> - Adapter

---

Specifies the target adapter.

**[-speed {1|2|4|8|10|auto}]** - Configured Speed

Specifies the adapter configuration speed in Gigabytes.

**[-state {down|up}]** - Configured State

Species the state of a target adapter. If up, the FCP port is online. If down, the FCP port is offline.

## Examples

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Configures the speed of FCP adapter 0d on node1 to 2 Gb/s.

## See Also

`network interface modify` `network fcp adapter show -instance`

---

## network fcp adapter show

Display FCP adapters

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

### Description

Displays FCP target adapter information. You can also use this information to determine if adapters are active and online.

The adapter argument is in the form Xy or Xy\_z where X and z are integers and y is a letter. An example is 4a or 4a\_1.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the FCP adapters that match this parameter value.

[-**adapter** <text>] - Adapter

Selects the FCP adapters that match this parameter value.

[-**description** <text>] - Description

Selects the FCP adapters that match this parameter value.

[-**physical-protocol** {fibre-channel|ethernet}] - Physical Protocol

Selects the FCP adapters that match this parameter value.

[-**max-speed** {1|2|4|8|10|auto}] - Maximum Speed

Selects the FCP adapters that match this parameter value.

[-**status** <text>] - Status

---

Selects the FCP adapters that match this parameter value.

**[-substatus <text>]** - Substatus

Selects the FCP adapters that match this parameter value. A substatus contains more detailed information than a status.

**[-portaddr <Hex Integer>]** - Host Port Address

Selects the FCP adapters that match this parameter value. This port address refers to the address assigned to the port by the fabric.

**[-firmware-rev <text>]** - Firmware Revision

Selects the FCP adapters that match this parameter value.

**[-data-link-rate <integer>]** - Data Link Rate (Gbit)

Selects the FCP adapters that match this parameter value.

**[-fabric-established {true|false}]** - Fabric Established

Selects the FCP adapters that match this parameter value. True displays all FCP adapters that are logged into the fabric. False displays all the FCP adapters that are not logged into the fabric.

**[-conn-established {loop|ptp}]** - Connection Established

Selects the FCP adapters that match this parameter value (loop or point-to-point loop).

**[-media-type {loop|ptp|auto}]** - Mediatype

Selects the FCP adapters that match this parameter value.

**[-speed {1|2|4|8|10|auto}]** - Configured Speed

Selects the FCP adapters that match this parameter value.

**[-state {down|up}]** - Configured State

Selects the FCP adapters that match this parameter value.

**[-switch-port <text>]** - Switch Port

Selects the FCP adapters that match this parameter value.

## Examples

```
cluster1::> fcp adapter show
Node      Adapter  Connection  Host
-----  -
node1     0d         loop       0
```

---

The example above displays information regarding FCP adapters within cluster1.

```
cluster1::> fcp adapter show -instance -node node1 -adapter 0d
      Node: node1
      Slot: 0d
      Description: Fibre Channel Target Adapter 0d (rev. 2)
Physical Protocol: fibre-channel
Maximum Speed: 4
      Status: link not connected
      Substatus: ADAPTER UP
Host Port Address: 0
Firmware Revision: 5.4.0
      PCI Bus Width: 64
      PCI Clock Speed: 33
      Cacheline Size: 16
      FC Packet Size: 2048
      SRAM Parity: true
      External GBIC: false
Data Link Rate (Gbit): 0
Fabric Established: false
Connection Established: loop
      Mediatype: ptp
      Configured Speed: auto
      Configured State: up
```

The example above displays detailed information regarding FCP adapter 0d in node1 within cluster1.



---

## network interface create

Create a logical interface

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

### Description

The `network interface create` command creates a logical interface (LIF).

Note:

Beginning with the Data ONTAP 8.0 Cluster-Mode family of releases, a logical interface is an IP address associated with a physical network port. For logical interfaces using NAS data protocols, the interface can fail over or be migrated to a different physical port in the event of component failures, thereby continuing to provide network access despite the component failure. Logical interfaces using SAN data protocols do not support migration or failover.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the Vserver on which the LIF is created.

**-lif** <lif-name> - Logical Interface Name

Use this parameter to specify the name of the LIF that is created. For iSCSI and FC LIFs, the name cannot be more than 254 characters.

**-role** {cluster|data|node-mgmt|intercluster|cluster-mgmt} - Role

Use this parameter to specify the role of the LIF. Typically, the role of the LIF matches the role of the network port on which the LIF is associated. A network port is the physical entity by which a LIF routes network traffic. Ports have four roles:

- Cluster ports, which provide communication among the nodes in a cluster
- Intercluster ports, which provide communication among peered clusters
- Data ports, which provide data access to NAS and SAN clients
- Node-management ports, which provide access to node management functionality.

---

LIFs with the cluster-management role behave as LIFs with the node-management role except that cluster-management LIFs can failover between nodes.

**[-data-protocol {nfs|cifs|iscsi|fc|fcache|none}, ...]** - Data Protocol

Use this parameter to specify the list of data protocols that can be configured on the LIF. The supported protocols are NFS, CIFS, FlexCache, iSCSI, and FCP. NFS, CIFS, and FlexCache are available by default when you create a LIF. If you specify "none", the LIF does not support any data protocols. Also, none, iscsi, or fcp cannot be combined with any other protocols.

Note:

The data-protocol field must be specified when the LIF is created and cannot be modified later.

**-home-node <nodename>** - Home Node

Use this parameter to specify the LIF's home node. The home node is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

**-home-port {<netport>|<ifgrp>}** - Home Port

Use this parameter to specify the LIF's home port or interface group. The home port is the port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.

**-address <IP Address>** - Network Address

Use this parameter to specify the LIF's IP address.

Note:

A cluster LIF cannot be on the same subnet as a management or data LIF.

**{ -netmask <IP Address> - Netmask**

Use this parameter to specify the LIF's netmask.

**| -netmask-length <integer> - Bits in the Netmask**

Use this parameter to specify the length (in bits) of the LIF's netmask.

**-auto {true|false} - IPv4 Link Local**

Use this parameter to specify whether IPv4 link local addressing is enabled for this LIF.

**[-routing-group <routing-group>]** - Routing Group Name

---

Use this parameter to specify the routing group, which enables multiple LIFs to share a set of routing table entries.

**[-status-admin {up|down}] - Administrative Status**

Use this parameter to specify whether the initial administrative status of the LIF is up or down. The default setting is `up`. The administrative status can differ from the operational status. For example, if you specify the status as `up` but a network problem prevents the interface from functioning, the operational status remains as `down`.

**[-failover-policy {nextavail|priority|disabled}] - Failover Policy**

Use this parameter to specify the failover policy for the LIF.

- `nextavail` - The LIF fails over to the next available physical port
- `priority` - The LIF fails over according to a failover rule.
- `disabled` - Failover is disabled for the LIF.

The failover policy for cluster ports is system-defined and cannot be changed. A default failover policy is assigned to data ports, but the default can be changed.

Note:

Logical interfaces for SAN protocols do not support failover. Thus, such interfaces will always show this parameter as `disabled`.

**[-firewall-policy <policy>] - Firewall Policy**

Use this parameter to specify the firewall policy for the LIF. A LIF can use a default firewall policy that corresponds to its role (management, cluster, intercluster, or data) or a custom firewall policy created by an administrator. View and modify existing firewall policies using the `system services firewall policy show` and `system services firewall policy modify` commands, respectively.

**[-auto-revert {true|false}] - Auto Revert**

Use this parameter to specify whether a data LIF is automatically reverted to its home node under certain circumstances. These circumstances include startup, when the status of the management database changes to either master or secondary, or when the network connection is made. The default setting is `false`. If you set the value of this parameter to `true`, load balancing migration capability of the data LIF is disabled (the `-allow-lb-migrate` parameter is set to `false`).

Note:

---

Logical interfaces for SAN traffic do not support auto-revert. Thus, this parameter is always `false` on such interfaces.

**[-dns-zone {zone-name|none}]** - Fully Qualified DNS Zone Name

Use this parameter to specify a unique, fully qualified domain name of a DNS zone to which this data LIF is added. You can associate a data LIF with a single DNS zone. All data LIFs included in a zone must be on the same Vserver. If a LIF is not added to a DNS zone the data LIF is created with the value `none`.

**[-listen-for-dns-query {true|false}]** - DNS Query Listen Enable

Use this parameter to specify if the LIF has to listen for DNS queries. The default value for this parameter is `true`.

**[-allow-lb-migrate {true|false}]** - Load Balancing Migrate Allowed (privilege: advanced)

Use this parameter to specify whether load balancing migration is activated for this data LIF. The default value of this parameter is `false`. If you set the value of this parameter to `true`, automatic revert capability for this data LIF is disabled (the `-auto-revert` parameter is set to `false`). Also, data LIFs that migrate as a result of load balancing adhere to network interface failover rules.

Note:

Load balancing migration takes effect only when there are no NFSv4, CIFS, or NRV connections.

**[-lb-weight <lb\_weight>]** - Load Balanced Weight (privilege: advanced)

Use this parameter to specify a load balancing weight for a data LIF. A valid load balancing weight is any integer between 1 and 100. When you specify the same load balancing weight for all data LIFs in a DNS zone, client requests are uniformly distributed, similar to round-robin DNS. A data LIF with a low load balancing weight is made available for client requests less frequently than one that has a high load balancing weight.

**[-failover-group <failover-group>]** - Failover Group Name

Use this parameter to specify the name of the failover group to associate with the LIF. Manage failover groups by using the `network interface failover-groups` command. A "clusterwide" failover group exists by default and includes all of the ports available in the cluster for failover. Furthermore, the failover group of the cluster-management LIF, which you specify when you create a cluster (see the `cluster create` command), is automatically set to "clusterwide".

Note:

---

Logical interfaces for SAN protocols do not support failover. Thus, this parameter cannot be specified for such interfaces.

**[-comment <text>]** - Comment

Use this parameter to specify the comment to associate with the LIF.

## Examples

The following example creates a LIF named `datalif1` on a Vserver named `vs0`. The LIF's home node is `node0` and its home port is `e0c`. The failover policy `nextavail` is assigned to the LIF, which has the IP address `192.0.2.130` and netmask `255.255.255.128`. The firewall policy is `data` and the LIF is automatically reverted to its home node at startup and under other circumstances.

```
cluster1::> network interface create -vserver vs0 -lif datalif1 -role data -  
home-node node0 -home-port e0c -address 192.0.2.130 -netmask 255.255.255.128 -  
failover-policy nextavail -firewall-policy data -auto-revert true
```

## See Also

`network interface revert`   `system services firewall policy show`  
`system services firewall policy modify`   `network interface failover-groups`  
`cluster create`

---

## network interface delete

Delete a logical interface

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

### Description

The `network interface delete` command deletes a logical interface from a Vserver.

Note:

If you are using SAN protocols and the LIF you want to delete is in a port set, you must remove the LIF from the port set before you can delete the LIF. To determine if a LIF is in a port set, use the `lun portset show` command. To remove the LIF from the port set, use the `lun portset remove` command.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the Vserver on which the logical interface to be deleted is located.

**-lif** <lif-name> - Logical Interface Name

Use this parameter to specify the logical interface to delete.

### Examples

The following example deletes a logical interface named `cluslif3` that is located on a Vserver named `vs0`.

```
cluster1::> network interface delete -vserver vs0 -lif cluslif3
```

### See Also

`lun portset show`   `lun portset remove`

---

## network interface migrate-all

Migrate all data and cluster management logical interfaces away from the specified node

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

### Description

The `network interface migrate-all` command migrates all data and cluster-management logical interfaces from the node you specify.

Note:

Manual migration of a logical interface can take up to 15 seconds to complete. Logical interface migration is a best-effort command and can only be completed if the destination node and port are operational. Logical interface migration requires that the logical interface be pre-configured with valid failover rules to facilitate failover to a remote node.

Note:

Logical interfaces for SAN protocols do not support migration. Attempts to do so will result in an error.

### Parameters

**-node** <nodename> - Node

Use this parameter to specify the node from which all logical interfaces are migrated. Each data and cluster-management logical interface is migrated to another node in the cluster, assuming that the logical interface is configured with failover rules that specify an operational node and port.

### Examples

The following example migrates all data and cluster management logical interfaces from the current (local) node.

```
node1::> network interface migrate-all -node local
```

---

## network interface migrate

Migrate a logical interface to a different port

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

### Description

The `network interface migrate` command migrates a logical interface to a port or interface group on the node you specify.

Note:

Manual migration of a logical interface can take up to 15 seconds to complete. Also, when you migrate a cluster logical interface, you must do so from the local node. Logical interface migration is a best-effort command, and can only be completed if the destination node and port are operational

Note:

Logical interfaces for SAN protocols do not support migration. Attempts to do so will result in an error.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the Vserver that owns the logical interface that is to be migrated.

**-lif** <lif-name> - Logical Interface Name

Use this parameter to specify the logical interface that is to be migrated.

**[-source-node** <nodename>] - Source Node

Use this parameter to specify the node from which the logical interface is to be migrated.

**-dest-node** <nodename> - Destination Node

Use this parameter to specify the node to which the logical interface is to be migrated.

**[-dest-port** {<netport>|<ifgrp>}] - Destination Port



---

Use this parameter to specify the port or interface group to which the logical interface is to be migrated.

**[-force [true]]** - Force Migrate Data LIF Flag (privilege: advanced)

Use this parameter to force the migration operation.

## Examples

The following example migrates a logical interface named `datalif1` on a Vserver named `vs0` to port `e0c` on a node named `node2`:

```
cluster1::> network interface migrate -vserver vs0 -lif datalif1 -source-node vs0  
-dest-node node2 -dest-port e0c
```

## network interface modify

Modify a logical interface

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

## Description

The `network interface modify` command modifies attributes of a logical interface (LIF).

Note:

You cannot modify some properties of an iSCSI or FCP LIF, such as `-home-node` or `-home-port`, if the LIF is in a port set. To modify these properties, first remove the LIF from the port set. To determine if a LIF is in a port set, use the `lun portset show` command. To remove the LIF from the port set, use the `lun portset remove` command.

## Parameters

**-vserver <vserver>** - Vserver Name

Use this parameter to specify the Vserver on which the LIF to be modified is located.

**-lif <lif-name>** - Logical Interface Name

Use this parameter to specify the name of the LIF that is to be modified

**[-home-node <nodename>]** - Home Node

---

Use this parameter to modify the LIF's home node. The home node is the node to which the LIF returns when the `network interface revert` command is run on that LIF.

**[-home-port {<netport>|<ifgrp>}]** - Home Port

Use this parameter to modify the LIF's home port. The home port is the port or interface group to which the LIF returns when the `network interface revert` command is run on that LIF.

Note:

If you change this parameter for a cluster or management LIF, you must reboot the storage system to force the change to take effect.

**[-address <IP Address>]** - Network Address

Use this parameter to modify the LIF's IP address.

Note:

A cluster LIF cannot be on the same subnet as a data or management LIF.

**{ [-netmask <IP Address>] - Netmask**

Use this parameter to modify the LIF's netmask.

**| [-netmask-length <integer>] - Bits in the Netmask**

Use this parameter to modify the length (in bits) of the LIF's netmask.

**[-auto {true|false}]** - IPv4 Link Local

Use this parameter to modify the LIF's IPv4 Link Local IP address.

**[-routing-group <routing-group>]** - Routing Group Name

Use this parameter to modify the routing group, which enables multiple LIFs to share a set of routing table entries.

**[-status-admin {up|down}]** - Administrative Status

Use this parameter to modify the administrative status of the LIF. The administrative status can differ from the operational status. For example, if you specify the status as `up` but a network problem prevents the interface from functioning, the operational status remains as `down`.

**[-failover-policy {nextavail|priority|disabled}]** - Failover Policy

Use this parameter to modify the failover policy for the LIF.

- `nextavail` - The LIF fails over to the next available physical interface.

- 
- `priority` - The LIF fails over according to a failover rule.
  - `disabled` - Failover is disabled for the LIF.

The failover policy for cluster ports is system-defined and cannot be changed. A default failover policy is assigned to data ports, but the default can be changed.

Note:

Logical interfaces for SAN protocols do not support failover. Thus, such interfaces always show this parameter as `disabled`.

#### **`[-firewall-policy <policy>]` - Firewall Policy**

Use this parameter to set the firewall policy for the LIF. A LIF can use a default firewall policy that corresponds to its role (management, cluster, or data) or a custom firewall policy created by an administrator. When using a custom policy, the interface will fallback on its role's default policy for unspecified services. View existing firewall policies with the `"system services firewall policy show"` command. Modify existing firewall policies with the `"system services firewall policy modify"` command.

#### **`[-auto-revert {true|false}]` - Auto Revert**

Use this parameter to modify whether a data LIF is reverted automatically to its home node under certain circumstances. These circumstances would include startup, when the status of the management database changes to either master or secondary, and when the network connection is made. The default setting is `false`. If you set the value of this parameter to `true`, the load balancing migration capability of the data LIF is disabled (the `-allow-lb-migrate` parameter is set to `false`).

Note:

Logical interfaces for SAN traffic do not support auto-revert. Thus, this parameter is always `false` on such interfaces.

#### **`[-dns-zone {zone-name|none}]` - Fully Qualified DNS Zone Name**

Use this parameter to modify the unique, fully qualified domain name of the DNS zone to which this data LIF belongs. You can associate a data LIF with a single DNS zone. All data LIFs included in a zone must be on the same Vserver. If you do not specify a value for this parameter, the data LIF is created with the value `none`.

#### **`[-listen-for-dns-query {true|false}]` - DNS Query Listen Enable**

Use this parameter to specify if the LIF has to listen for DNS queries. The default value for this parameter is `true`.

---

**[-allow-lb-migrate {true|false}]** - Load Balancing Migrate Allowed (privilege: advanced)

Use this parameter to modify whether or not load balancing migration is enabled for this data LIF. The default value of this parameter is `false`. If you set the value of this parameter to `true`, the automatic revert capability of the data LIF is disabled (the `-auto-revert` parameter is set to `false`). Also, data LIFs that migrate as a result of load balancing adhere to network interface failover rules.

Note:

Load balancing migration will only take effect when there are no NFSv4, CIFS, or NRV connections.

**[-lb-weight <lb\_weight>]** - Load Balanced Weight (privilege: advanced)

Use this parameter to modify the load balancing weight of the data LIF. A valid load balancing weight is any integer between 1 and 100. If you specify the same load balancing weight for all data LIFs in a DNS zone, client requests are uniformly distributed, similar to round-robin DNS. A data LIF with a low load balancing weight is made available for client requests less frequently than one that has a high load balancing weight.

**[-failover-group <failover-group>]** - Failover Group Name

Use this parameter to modify the name of the failover group to associate with the network interface. Create failover groups using the `network interface failover create` command. A "clusterwide" failover group exists by default and includes all of the ports available in the cluster for LIF failover. Furthermore, the failover group of the cluster management LIF, which you specify when you create a cluster (see the `cluster create` command), is automatically set to "clusterwide".

Note:

Logical interfaces for SAN protocols do not support failover. Thus, this parameter cannot be specified for such interfaces.

**[-comment <text>]** - Comment

Use this parameter to modify the comment associated with the LIF.

## Examples

The following example modifies a LIF named `datalif1` on a logical server named `vs0`. The LIF's netmask is modified to `255.255.255.128`.

```
cluster1::> network interface modify -vserver vs0 -lif datalif1 -netmask
255.255.255.128
```

---

## See Also

network interface revert   system services firewall policy show  
system services firewall policy modify   network interface failover create   cluster create  
lun portset show   lun portset remove

---

## network interface rename

Rename a logical interface

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

### Description

Use the `network interface rename` command to change the name of an existing logical interface.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the Vserver on which the logical interface to rename is located.

**-lif** <lif-name> - Logical Interface Name

Use this parameter to specify the name of the logical interface to rename.

**-newname** <text> - LIF

Use this parameter to specify the new name of the logical interface. For iSCSI and FC LIFs, the name cannot be more than 254 characters.

### Examples

The following example renames a cluster logical interface named `cluslif1` to `cluslif4` on a Verver named `vs0`.

```
cluster1::> network interface rename -vserver vs0 -lif cluslif1 -newname cluslif4
```

## network interface revert

Revert a logical interface to its home port

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

### Description

---

The `network interface revert` command reverts a logical interface that is not currently on its home port to its home port, assuming that the home node and port are both operational. A logical interface's home port is specified when the logical interface is created. Determine a logical interface's home port by using the `network interface show` command.

## Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the Vserver on which the logical interface to be reverted is located.

**-lif** <lif-name> - Logical Interface Name

Use this parameter to specify the logical interface that is to be reverted.

Note:

Logical interfaces for SAN protocols are always home. Thus, this command has no effect on such interfaces. The same applies to logical interfaces for NAS protocols that are already home.

## Examples

The following example returns any logical interfaces that are not currently on their home ports to their home ports.

```
cluster1::> network interface revert -vserver * -lif *
```

## See Also

`network interface show`

---

# network interface show-routing-group

Show the logical interfaces for each Vserver and routing group

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

## Description

The `network interface show-routing-group` command displays the logical interfaces for each Vserver and routing group.

## Parameters

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

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

| [-instance ] }

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

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

Use this parameter plus the `-lif` parameter to display detailed information only about the logical interface you specify.

**[-lif <lif-name>]** - Logical Interface Name

Use this parameter plus the `-vserver` parameter to display detailed information only about the logical interface you specify.

**[-routing-group <routing-group>]** - Routing Group Name

Use this parameter to display only information about the routing groups you specify.

## Examples

The following example shows the logical interfaces for each Vserver and routing group.

```
cluster1::> network interface show-routing-group
Vserver      Routing Group      Interface Name
-----
vs_ie1
              d172.17.176.120/24    data1
              d172.17.176.120/24    data2
ie3070-2
              c172.17.177.122/24    clus1
```



---

	c172.17.177.122/24	clus1
	c172.17.177.122/24	clus2
ie3070-1	n172.17.178.122/24	mgmt1
	c172.17.177.120/24	clus1
	c172.17.177.120/24	clus2
ie3070-3	n172.17.178.120/24	mgmt1
	c172.17.177.124/24	clus1
	c172.17.177.124/24	clus2
ie3070-4	n172.17.178.124/24	mgmt1
	c172.17.177.126/24	clus1
	c172.17.177.126/24	clus1
	n172.17.178.126/24	mgmt1

14 entries were displayed.

---

## network interface show-zones

Show the DNS zone names of LIFs

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

### Description

The `network interface show-zones` command displays information about logical interfaces and whether the interface is associated with a Domain Name System (DNS) load balancing zone.

### Parameters

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

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

| [-**instance** ] }

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

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

Use this parameter to display information only about logical interfaces on the Vserver you specify.

Use this parameter plus the `-lif` parameter to display information only about the logical interface you specify.

[-**lif** <lif-name>] - Logical Interface Name

Use this parameter to display information only about logical interfaces that match the name you specify.

Use this parameter with the `-vserver` parameter to display information only about the logical interface you specify.

[-**dns-zone** {zone-name|none}] - Fully Qualified DNS Zone Name

Use this parameter to display only information about logical interfaces that are associated with the DNS zone you specify.

---

## **[`-listen-for-dns-query` {true|false}] - DNS Query Listen Enable**

Use this parameter to display information about logical interfaces which are either listening or not listening for DNS queries.

### **Examples**

The following example displays general information about all logical interfaces and DNS zones.

```
cluster1::> network interface show-zones
```

Vserver	Interface Name	DNS Zone	Listen For DNS Query
vs1	data1	www.example1.com	true
	data2	www.example1.com	false
vs2	data1	www.example2.com	true
	data2	www.example2.com	true
node1	clus1	none	false
	clus2	none	false
	mgmt1	none	false
node2	clus1	none	false
	clus2	none	false
	mgmt1	none	false
cluster	cluster_mgmt	none	false

11 entries were displayed.

---

## network interface show

Display logical interfaces

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

### Description

The `network interface show` command displays information about logical interfaces.

Running the command with the `-failover` parameter displays information relevant to logical interface failover rules. See the examples for more information.

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about logical interfaces whose operational status is down, run the command with the `-status-oper down` parameter.

### Parameters

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

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

| **[-failover ]**

Use this parameter to display logical-interface failover information.

| **[-instance ] }**

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

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

Use this parameter to display information only about logical interfaces on the Vserver you specify.

Use this parameter plus the `-lif` parameter to display detailed information only about the logical interface you specify.

**[-lif <lif-name>]** - Logical Interface Name

Use this parameter to display information only about logical interfaces that match the name you specify.

---

Use this parameter with the `-vserver` parameter to display detailed information only about the logical interface you specify.

**`[-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}]`** - Role

Use this parameter to display information only about logical interfaces that are associated with network ports that have the role you specify.

**`[-data-protocol {nfs|cifs|iscsi|fc|fcache|none}, ...]`** - Data Protocol

Use this parameter to display information only about logical interfaces that have the enabled data protocols you specify.

**`[-home-node <nodename>]`** - Home Node

Use this parameter to display information only about logical interfaces that have the home node you specify.

**`[-home-port {<netport>|<ifgrp>}]`** - Home Port

Use this parameter to display information only about logical interfaces that have the home port or interface group you specify.

**`[-curr-node <nodename>]`** - Current Node

Use this parameter to display information only about logical interfaces that are currently located on the node you specify.

**`[-curr-port {<netport>|<ifgrp>}]`** - Current Port

Use this parameter to display information only about logical interfaces that are currently located on the port or interface group you specify.

**`[-status-oper {up|down}]`** - Operational Status

Use this parameter to display information only about logical interfaces that have the operational status you specify.

**`[-status-extended <text>]`** - Extended Status

Use this parameter to display information only about logical interfaces that match the extended status that you specify. This applies only to FCP logical interfaces.

**`[-numeric-id <integer>]`** - Numeric ID (privilege: advanced)

Use this parameter to display information only about logical interfaces with the numeric ID (or range of IDs) you specify. The numeric ID is an integer that identifies the logical interface in the cluster.

**`[-is-home {true|false}]`** - Is Home

---

Use this parameter to display information only about logical interfaces that are (true) or are not (false) currently located on their home node and port.

**[-address <IP Address>]** - Network Address

Use this parameter to display information only about logical interfaces that match the IP address or address range you specify.

**[-netmask <IP Address>]** - Netmask

Use this parameter to display information only about logical interfaces that have the netmask you specify.

**[-netmask-length <integer>]** - Bits in the Netmask

Use this parameter to display information only about logical interfaces with a netmask that has the number of bits you specify.

**[-auto {true|false}]** - IPv4 Link Local

Use this parameter to display information only about logical interfaces that have IPv4 link local IP addresses.

**[-routing-group <routing-group>]** - Routing Group Name

Use this parameter to display information only about logical interfaces that are in the routing group you specify. Logical interfaces in a routing group share a set of routing table entries.

**[-status-admin {up|down}]** - Administrative Status

Use this parameter to display information only about logical interfaces that have the administrative status you specify.

**[-failover-policy {nextavail|priority|disabled}]** - Failover Policy

Use this parameter to display information only about logical interfaces that use the failover policy you specify.

**[-firewall-policy <policy>]** - Firewall Policy

Use this parameter to display information only about logical interfaces that use the firewall policies you specify.

**[-auto-revert {true|false}]** - Auto Revert

Use this parameter to display information only about logical interfaces that have auto-revert setting you specify.

**[-sticky {true|false}]** - Sticky Flag (privilege: advanced)

Use this parameter to display information only about logical interfaces that are "sticky". A sticky logical interface is one that has been manually migrated to another node and

---

is not subject to auto-revert settings. A sticky logical interface remains at the migrated location until it is manually reverted or until it fails over to another node.

**[-dns-zone {zone-name|none}]** - Fully Qualified DNS Zone Name

Use this parameter to display information only about logical interfaces in the specified DNS zone.

**[-listen-for-dns-query {true|false}]** - DNS Query Listen Enable

Use this parameter to display information only about logical interfaces that have the DNS query listen value you specify.

**[-allow-lb-migrate {true|false}]** - Load Balancing Migrate Allowed (privilege: advanced)

Use this parameter to display information only about logical interfaces for which load balancing migration is activated (true) or not activated (false).

**[-lb-weight <lb\_weight>]** - Load Balanced Weight (privilege: advanced)

Use this parameter to display information only about logical interfaces that have the load balancing weight you specify.

**[-failover-group <failover-group>]** - Failover Group Name

Use this parameter to display information only about logical interfaces that are in the failover group you specify. Logical interfaces in the same failover group are capable of failing over to the same set of ports.

**[-address-family {ipv4|ipv6|ipv6z}]** - Address family

Use this parameter to view the address family that is in use on the interface. Only IPv4 and IPv6 non-zoned addresses can be configured. Configuration of IPv6z addresses is not allowed.

**[-comment <text>]** - Comment

Use this parameter to display information only about logical interfaces that have the comment you specify.

## Examples

The following example displays general information about all logical interfaces.

```
cluster1::> network interface show
Vserver      Logical   Status   Network   Current   Current   Is
-----      -
node0         cluslif1  up/up    192.0.2.66/192  node0     e0a       true
              cluslif2  up/up    192.0.2.67/192  node0     e0b       true
              mgmtlif1  up/up    192.0.2.2/192   node0     e1a       true
node1         cluslif1  up/up    192.0.2.68/192  node1     e0a       true
              cluslif2  up/up    192.0.2.69/192  node1     e0b       true
              mgmtlif1  up/up    192.0.2.3/192   node1     e1a       true
```

---

node2	cluslif1	up/up	192.0.2.70/192	node2	e0a	true
	cluslif2	up/up	192.0.2.71/192	node2	e0b	true
	mgmtlif1	up/up	192.0.2.4/192	node2	e1a	true
node3	cluslif1	up/up	192.0.2.72/192	node3	e0a	true
	cluslif2	up/up	192.0.2.73/192	node3	e0b	true
	mgmtlif1	up/up	192.0.2.5/192	node3	e1a	true

The following example displays failover information about all logical interfaces.

```
cluster1::> network interface show -failover
```

Vserver	Logical Interface	Failover Policy	Home Node	Home Port	Current Node	Current Port
-----						
node0	cluslif1	nextavail	node0	e0a	node0	e0a
	cluslif2	nextavail	node0	e0b	node0	e0b
	mgmtlif1	nextavail	node0	e1a	node0	e1a
node1	cluslif1	nextavail	node1	e0a	node1	e0a
	cluslif2	nextavail	node1	e0b	node1	e0b
	mgmtlif1	nextavail	node1	e1a	node1	e1a
node2	cluslif1	nextavail	node2	e0a	node2	e0a
	cluslif2	nextavail	node2	e0b	node2	e0b
	mgmtlif1	nextavail	node2	e1a	node2	e1a
node3	cluslif1	nextavail	node3	e0a	node3	e0a
	cluslif2	nextavail	node3	e0b	node3	e0b
	mgmtlif1	nextavail	node3	e1a	node3	e1a



---

## network interface start-cluster-check

Start the cluster check function

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

### Description

The `network interface start-cluster-check` command initiates an accessibility check from every logical interface to every aggregate. Automatic checks run periodically, but this command manually initiates a check immediately.

This command produces no direct output. Any errors encountered during the check are reported in the event log. See the `event log show` command for more information.

### Parameters

None

### Examples

This example shows an execution of this command, with all parameters and output.

```
cluster1::> network interface start-cluster-check
```

### See Also

`event log show`

---

## network interface failover-groups create

Create a new failover group or add an entry to an existing group

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

### Description

The `network interface failover-groups create` command creates a grouping of failover targets for logical interfaces on one or more nodes. Use this command to add a new network port or an interface group to an existing failover group.

Note:

Interfaces for SAN protocols do not support failover. Such interfaces are not valid failover targets.

### Parameters

**-failover-group** <text> - Failover Group Name

The name of the logical interface failover group that you want to create or extend.

**-node** <nodename> - Node

The node on which the failover target (a network port or interface group) is located.

**-port** <netport> - Port

The network port or interface group to be added to the group.

### Examples

The following example shows how to create a failover group named `failover-group_2` containing port `e1e` on node `Xena`.

```
cluster1::> network interface failover-groups create -failover-group failover-group_2 -node xena -port e1e
```

The following example shows how to extend an existing failover group named `failover-group_2` to also contain port `e2e` on node `Xena`.

```
cluster1::> network interface failover-groups create -failover-group failover-group_2 -node xena -port e2e
```

---

## network interface failover-groups delete

Remove a port from a failover group

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

### Description

The `network interface failover-groups delete` command removes a failover target (a network port or interface group) from an existing failover group. Use this command with the `-failover-group` parameter and the name of an existing logical interface failover group plus either the `node` parameter or the `port` parameter and the value "\*" to delete the entire logical-interface failover group.

### Parameters

**-failover-group** <text> - Failover Group Name

Use this parameter to specify the name of the logical interface failover group.

**-node** <nodename> - Node

Use this parameter to specify the node on which the failover target is located.

**-port** <netport> - Port

Use this parameter to specify the network port or port interface group to be removed from the failover group.

### Examples

The following example shows how to delete a failover group named `failover-group_2` containing port `e1e` on node `Xena`.

```
cluster1::> network interface failover-groups delete -failover-group failover-group_2 -node xena -port e1e
```

## network interface failover-groups rename

Rename a logical interface failover group

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

---

## Description

The `network interface failover-groups rename` command enables you to rename an existing group of failover rules.

## Parameters

**-failover-group** <text> - Failover Group Name

Use this parameter to specify the failover group that you want to rename.

**-new-name** <text> - New Failover Group Name

Use this parameter to specify the new name of the failover group.

## Examples

This example shows the failover group "clusterwide" being renamed "clyde".

```
cluster1::> network interface failover-group rename -failover -group clusterwide  
-new-name clyde
```

## network interface failover-groups show

Display logical interface failover groups

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

## Description

The `network interface failover-groups show` command displays information about logical interface failover groups.

## Parameters

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

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

| [-instance ] }

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

---

**[-failover-group <text>]** - Failover Group Name

Selects the failover groups that match this parameter value

Use this parameter with the `-node` parameter and the `-port` parameter to display information only about the individual logical interface failover group you specify.

**[-node <nodename>]** - Node

Selects the failover groups that match this parameter value

**[-port <netport>]** - Port

Selects the failover groups that match this parameter value

## Examples

The following example displays information about all logical interface failover groups on a two-node cluster.

```
cluster1::> network interface failover groups show
Failover
Group      Node      Port
-----
clusterwide
           gabrielle e0c
           gabrielle e0d
           gabrielle e1b
           gabrielle e1c
           gabrielle e1d
           xena     e0c
           xena     e0d
           xena     e1b
           xena     e1c
           xena     e1d
10 entries were displayed
```

---

## network options ipv6 modify

Modify IPv6 options

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

### Description

This command sets the state of IPv6 options for the cluster.

### Parameters

**[-enabled [true]]** - IPv6 Enabled

Setting this parameter to true enables IPv6 for the cluster. IPv6 cannot be disabled once it is enabled for the cluster. Call technical support for guidance regarding disabling IPv6.

### Examples

```
cluster1::*> network options ipv6 modify -enabled true
```

## network options ipv6 show

Display IPv6 options

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

### Description

This command displays the current state of IPv6 options for the cluster.

### Parameters

None

### Examples

```
cluster1::*> network options ipv6 show
IPv6 Enabled: false
```

---

## network options switchless-cluster modify

Modify switchless cluster network options

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

### Description

This command sets whether the cluster network is in switchless or switched mode. A switchless cluster is physically formed by connecting two nodes back-to-back, without a switch between them.

### Parameters

**[-enabled {true|false}]** - Enable Switchless Cluster (privilege: advanced)

This parameter specifies whether the switchless cluster is enabled or not. Setting this parameter to true enables the switchless cluster.

### Examples

The following example enables the switchless cluster:

```
cluster1::*> network options switchless-cluster modify -enabled true
```

## network options switchless-cluster show

Display switchless cluster network options

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

### Description

The network options switchless-cluster show command displays the attributes of a switchless cluster.

### Parameters

None

### Examples

---

The following example displays the attributes of the switchless cluster:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: true
```



---

## network port delete

Delete a network port

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

### Description

The `network port delete` command deletes a network port.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the port is located.

**-port** {<netport>|<ifgrp>} - Port

This specifies the port to delete.

### Examples

The following example deletes port e0c from a node named node0. The commands works only when the port is down.

```
cluster1::> network port delete -node node0 -port e0c
```

## network port modify

Modify network port attributes

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

### Description

The `network port modify` command enables you to change the maximum transmission unit (MTU) setting, autonegotiation setting, administrative duplex mode, and administrative speed of a specified network port.

### Parameters

**-node** {<nodename>|local} - Node

---

Use this parameter to specify the node on which the port is located.

**-port** {<netport>|<ifgrp>} - Port

Use this parameter to specify the port that you want to modify.

**[-role** {cluster|data|node-mgmt|intercluster|cluster-mgmt}] - Role

The port's role: cluster (for cluster communication between nodes), data (for client access to data), node management (for managing a node), or intercluster (for communicating with a different cluster). cluster-mgmt is not a supported port role.

Note:

Changing a port's role automatically removes the port from the failover rules and failover groups associated with the port's old role.

**[-mtu** <integer>] - MTU

The port's MTU setting. The default setting when you create a port is 9000.

**[-autonegotiate-admin** {true|false}] - Auto-Negotiation Administrative

Whether the port uses Ethernet autonegotiation to determine the highest speed and duplex mode that the port and its endpoint can support. The default setting when you create a port is `true`.

**[-duplex-admin** {auto|half|full}] - Duplex Mode Administrative

The administrative setting for the port's duplex mode. This is the duplex mode that you prefer the port to use. Depending on network limitations, the operational value can be different from the administrative setting. The default setting when you create a port is `full`.

**[-speed-admin** {auto|10|100|1000|10000}] - Speed Administrative

The administrative speed setting, in megabits per second. This is the speed setting that you prefer the port to use. Depending on network limitations, the operational value can be lower than the administrative setting.

**[-flowcontrol-admin** {none|receive|send|full}] - Flow Control Administrative

The administrative flow control setting of the port. this is the flow control setting that you prefer the port to use. Depending on network and port limitations, the operational value can be different from the administrative setting.

**[-up-admin** {true|false}] - Up Administrative (privilege: advanced)

The administrative state of the port. If set to `true`, the port is used if it is operational. If set to `false`, the port is configured down.

---

## Examples

The following example modifies port e0a on a node named node0 not to use auto-negotiation, to preferably use half duplex mode, and to preferably run at 100 Mbps.

```
cluster1::> network port modify -node node0 -port e0a -autonegotiate-admin false
-duplex-admin half -speed-admin 100
```

## network port show

Display network port attributes

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

## Description

The `network port show` command displays information about network ports. The command output indicates any inactive links, and lists the reason for the inactive status.

Some parameters can have "administrative" and "operational" values. The administrative setting is the preferred value for that parameter, which is set when the port is created or modified. The operational value is the actual current value of that parameter. For example, if the network is underperforming due to network problems, the operational speed value can be lower than the administrative setting.

If the operational duplex mode and speed of a port cannot be determined (for instance, if the link is down), that port's status is listed as `undef`, meaning undefined.

## Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Selects the network ports that match this parameter value. Use this parameter with the `-port` parameter to select a port.

---

**[-port {<netport>|<ifgrp>}]** - Port

Selects the network ports that match this parameter value. If you do not use this parameter, the command displays information about all network ports.

**[-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}]** - Role

Selects the network ports that match this parameter value. For example, to display information about all management ports in the cluster, run the command with the parameter `-role` set to `node-mgmt`. Note that `cluster-mgmt` is not a supported port role.

**[-link {off|up|down}]** - Link

Selects the network ports that match this parameter value.

**[-mtu <integer>]** - MTU

Selects the network ports that match this parameter value.

**[-autonegotiate-admin {true|false}]** - Auto-Negotiation Administrative

Selects the network ports that match this parameter value.

**[-autonegotiate-oper {true|false}]** - Auto-Negotiation Operational

Selects the network ports that match this parameter value.

**[-duplex-admin {auto|half|full}]** - Duplex Mode Administrative

Selects the network ports that match this parameter value.

**[-duplex-oper {auto|half|full}]** - Duplex Mode Operational

Selects the network ports that match this parameter value.

**[-speed-admin {auto|10|100|1000|10000}]** - Speed Administrative

Selects the network ports that match this parameter value.

**[-speed-oper {auto|10|100|1000|10000}]** - Speed Operational

Selects the network ports that match this parameter value.

**[-flowcontrol-admin {none|receive|send|full}]** - Flow Control Administrative

Selects the network ports that match this parameter value.

**[-flowcontrol-oper {none|receive|send|full}]** - Flow Control Operational

Selects the network ports that match this parameter value.

**[-mac <MAC Address>]** - MAC Address

Selects the network ports that match this parameter value.

---

**[-up-admin {true|false}]** - Up Administrative (privilege: advanced)

Selects the network ports that match this parameter value.

**[-type {physical|if-group|vlan}]** - Port Type

Selects the network ports that match this parameter value.

**[-ifgrp-node <nodename>]** - Interface Group Parent Node

Selects the network ports that match this parameter value.

**[-ifgrp-port {<netport>|<ifgrp>}]** - Interface Group Parent Port

Selects the network ports that match this parameter value.

**[-ifgrp-distr-func {mac|ip|sequential|port}]** - Distribution Function

Selects the network ports that match this parameter value.

**[-ifgrp-mode {multimode|multimode\_lacp|singlemode}]** - Create Policy

Selects the network ports that match this parameter value.

**[-vlan-node <nodename>]** - Parent VLAN Node

Selects the network ports that match this parameter value.

**[-vlan-port {<netport>|<ifgrp>}]** - Parent VLAN Port

Selects the network ports that match this parameter value.

**[-vlan-tag <integer>]** - VLAN Tag

Selects the network ports that match this parameter value.

**[-remote-device-id <text>]** - Remote Device ID

Selects the network ports that match this parameter value.

## Examples

The following example displays information about all network ports.

```
cluster1::> network port show
```

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node0	e0a	cluster	up	9000	true/true	full/full	1000/1000
	e0b	cluster	up	9000	true/true	full/full	1000/1000
	e0c	data	up	1500	true/true	full/full	1000/1000
	e0d	data	up	1500	true/true	full/full	1000/1000
	e1a	mgmt	up	1500	true/true	full/full	1000/1000
node1	e0a	cluster	up	9000	true/true	half/full	10/1000
	e0b	cluster	up	9000	true/true	half/full	10/1000
	e0c	data	up	1500	true/true	half/full	10/1000
	e0d	data	up	1500	true/true	half/full	10/1000
	e1a	mgmt	up	1500	true/true	full/full	1000/1000
node2							

---

	e0a	cluster	up	9000	true/true	full/full	auto/1000
	e0b	cluster	up	9000	true/true	full/full	auto/1000
	e0c	data	up	1500	true/true	full/full	auto/1000
	e0d	data	up	1500	true/true	full/full	auto/1000
node3	e1a	mgmt	up	1500	true/true	full/full	auto/1000
	e0a	cluster	up	9000	true/true	full/full	auto/1000
	e0b	cluster	up	9000	true/true	full/full	auto/1000
	e0c	data	up	1500	true/true	full/full	auto/1000
	e0d	data	up	1500	true/true	full/full	auto/1000
	e1a	mgmt	up	1500	true/true	full/full	auto/1000

---

## network port ifgrp add-port

Add a port to an interface group

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

### Description

The `network port ifgrp add-port` command adds a network port to a port interface group. The port interface group must already exist. You can create a port interface group by using the `network port ifgrp create` command.

The following restrictions apply to port interface groups:

- A port that is already a member of a port interface group cannot be added to another port interface group.
- All ports in a port interface group must have the same port role (data).
- Cluster ports and management ports cannot be in a port interface group.
- A port to which a logical interface is already bound cannot be added to a port interface group.
- A port that already has an assigned failover role cannot be added to a port interface group.
- All ports in a port interface group must be physically located on the same node.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the port interface group is located.

**-ifgrp** {<netport>|<ifgrp>} - Interface Group Name

The port interface group to which a port is to be added.

**-port** <netport> - Specifies the name of port.

The network port that is to be added to the port interface group.

### Examples

The following example adds port e0c to port interface group a1a on a node named node1:

---

```
cluster1::> network port ifgrp add-port -node node1 -ifgrp ala -port e0c
```

## See Also

[network port ifgrp create](#)



---

## network port ifgrp create

Create a port interface group

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

### Description

The `network port ifgrp create` command creates a port interface group. See the documentation for the `network port ifgrp add-port` command for a list of restrictions on creating port interface groups.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the port interface group will be created.

**-ifgrp** {<netport>|<ifgrp>} - Interface Group Name

The name of the port interface group that will be created. Port interface groups must be named using the syntax "a<number><letter>", where <number> is an integer in the range [0-999] without leading zeros and <letter> is a lowercase letter. For example, "a0a", "a0b", "a1c", and "a2a" are all valid port interface group names.

**-distr-func** {mac|ip|sequential|port} - Distribution Function

The distribution function of the port interface group that will be created. Valid values are:

- mac - Network traffic is distributed based on MAC addresses
- ip - Network traffic is distributed based on IP addresses
- sequential - Network traffic is distributed as it is received
- port - Network traffic is distributed evenly across all member ports of the interface group

**-mode** {multimode|multimode\_lacp|singlemode} - Create Policy

The create policy for the interface group that will be created. Valid values are:

- multimode - Bundle multiple member ports of the interface group to act as a single trunked port

- 
- `multimode_lacp` - Bundle multiple member ports of the interface group using Link Aggregation Control Protocol
  - `singlemode` - Provide port redundancy using member ports of the interface group for failover

## Examples

The following example creates a port interface group named `a0a` on node `node0` with a distribution function of `ip`:

```
cluster1::> network port ifgrp create -node node0 -ifgrp a0a -distr-func ip -mode  
multimode
```

## See Also

`network port ifgrp add-port`

---

## network port ifgrp delete

Destroy a port interface group

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

### Description

The `network port ifgrp delete` command destroys a port interface group. Before deleting a port interface group, remove all ports from it with the `network port ifgrp remove-port` command.

Note:

When you delete an interface group port, it is automatically removed from failover rules and groups to which it belongs.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the port interface group is located.

**-ifgrp** {<netport>|<ifgrp>} - Interface Group Name

The port interface group that will be deleted.

### Examples

The following example deletes port interface group a0b from a node named node0.

```
cluster1::> network port ifgrp delete -node node0 -ifgrp a0b
```

### See Also

`network port ifgrp remove-port`

---

## network port ifgrp remove-port

Remove a port from an interface group

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

### Description

The `network port ifgrp remove-port` command removes a network port from a port interface group.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the port interface group is located.

**-ifgrp** {<netport>|<ifgrp>} - Interface Group Name

The port interface group from which a port will be removed.

**-port** <netport> - Specifies the name of port.

The network port that will be removed from the port interface group.

### Examples

The following example removes port e0d from port interface group a1a on a node named node1:

```
cluster1::> network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

## network port ifgrp show

Display port interface groups

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

### Description

The `network port ifgrp show` command displays information about port interface groups. By default, it displays information about all port interface groups on all nodes in the cluster.

---

## Parameters

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

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

**| [-instance ] }**

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

**[-node {<nodename>|local}]** - Node

Selects the port interface groups that match this parameter value. Use this parameter with the `-ifgrp` parameter to select information about a specific port interface group.

**[-ifgrp {<netport>|<ifgrp>}]** - Interface Group Name

Selects the port interface groups that match this parameter value. Use this parameter with the `-node` parameter, to select information about a specific port interface group.

**[-distr-func {mac|ip|sequential|port}]** - Distribution Function

Selects the port interface groups that match this parameter value.

**[-mode {multimode|multimode\_lacp|singlemode}]** - Create Policy

Selects the port interface groups that match this parameter value.

**[-mac <MAC Address>]** - MAC Address

Selects the port interface groups that match this parameter value.

**[-activeports {full|partial|none}]** - Port Participation

Selects the port interface groups that match this parameter value. The value "partial" indicates that some but not all of the port interface group's ports are active. the value "full" indicates that all of the port interface group's ports are active.

**[-ports {<netport>|<ifgrp>}, ...]** - Network Ports

Selects the port interface groups that match this parameter value.

**[-up-ports {<netport>|<ifgrp>}, ...]** - Up Ports

Selects the port interface groups that match this parameter value. Displays only the ports that are up.

**[-down-ports {<netport>|<ifgrp>}, ...]** - Down Ports

---

Selects the port interface groups that match this parameter value. Displays only the ports that are down.

**Examples**

The following example displays information about all port interface groups.

```
cluster1::> network port ifgrp show
Node      Port      Distribution      MAC Address      Active      Ports
-----  -
node0     a0a       ip               b8:f8:7a:20:00   partial    e0c
node1     ala       ip               07:26:60:02:00   full       e0d
```

---

## network port vlan create

Create a virtual LAN (VLAN)

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

### Description

The `network port vlan create` command attaches a VLAN to a network port on a specified node.

### Parameters

**-node** {<nodename>|local} - Node

The node to which the VLAN is to be attached.

Note:

You cannot attach a VLAN to a cluster port.

{ **-vlan-name** {<netport>|<ifgrp>} - VLAN Name

The name of the VLAN that is to be attached. This name should be a combination of the name of the port or interface group and the VLAN ID, with a hyphen between, such as "e1c-80".

| **-port** {<netport>|<ifgrp>} - Associated Network Port

The network port to which the VLAN is to be attached.

**-vlan-id** <integer> } - Network Switch VLAN Identifier

The ID tag of the created VLAN.

### Examples

This example shows how to create VLAN e1c-80 attached to network port e1c on node1.

```
cluster1::> network port vlan create -node node1 -vlan-name e1c-80
```

## network port vlan delete

---

Delete a virtual LAN (VLAN)

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

## Description

The `network port vlan delete` command deletes a VLAN from a network port.

Note:

When you delete a VLAN port, it is automatically removed from all failover rules and groups that use it.

## Parameters

**-node** {<nodename>|local} - Node

The node from which the VLAN is to be deleted.

{ **-vlan-name** {<netport>|<ifgrp>} - VLAN Name

The name of the VLAN that is to be deleted

| **-port** {<netport>|<ifgrp>} - Associated Network Port

The network port to which the VLAN is to be attached.

**-vlan-id** <integer> } - Network Switch VLAN Identifier

The ID tag of the deleted VLAN.

## Examples

This example shows how to delete VLAN e1c-80 from network port e1c on node1.

```
cluster1::> network port vlan delete -node node1 -vlan-name e1c-80
```

## network port vlan show

Display virtual LANs (VLANs)

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

## Description



---

The `network port vlan show` command displays information about network ports that are attached to VLANs. The command output indicates any inactive links and lists the reason for the inactive status.

If the operational duplex mode and speed cannot be determined (for instance, if the link is down), they are listed as `undef`, meaning undefined.

## Parameters

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

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

| **[-instance ]** }

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

**[-node {<nodename>|local}]** - Node

Selects the VLAN network ports that match this parameter value.

{ **[-vlan-name {<netport>|<ifgrp>}]** - VLAN Name

Selects the VLAN network ports that match this parameter value.

| **[-port {<netport>|<ifgrp>}]** - Associated Network Port

Selects the VLAN network ports that match this parameter value. If neither this parameter nor `-name` are used, the command displays information about all network ports.

**[-vlan-id <integer>]** } - Network Switch VLAN Identifier

Selects the VLAN network ports that match this parameter value.

**[-mac <MAC Address>]** - MAC address

Selects the VLAN network ports that match this parameter value.

## Examples

The example below shows VLAN e1b-70 attached to port e1b on node1.

```
cluster1::> network port vlan show
              Network Network
Node  VLAN Name  Port  VLAN ID  MAC Addresss
-----
node1  e1b-70    e1b    70      00:15:17:76:7b:69
```

---

## network routing-groups create

Create a routing group

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

### Description

The `network routing-groups create` command creates a group of static routes. After you have created a routing group, you can add routes to the group by using the `network routing-groups route create` command.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies the node or Vserver on which the routing group will be created.

**-routing-group** <text> - Routing Group

Specifies the name of the routing group that you want to create.

**-subnet** <IpAddress/Mask> - Address/Mask

Specifies the IP address and subnet mask of the routing group's destination. The format for this value is: address, slash ("/"), mask. The example below has `192.0.2.165/24` as a valid value for the `-subnet` parameter.

**-role** {cluster|data|node-mgmt|intercluster|cluster-mgmt} - Role

Defines the role of the routing group. The routing group can be a cluster, data, node management, intercluster, or cluster management routing group. There is no default.

**[-metric** <integer>] - Metric

Specifies a hop count for the routing group that you are creating. The default is 20.

### Examples

The following example creates a routing group for data from the Vserver node1 with an IP address of 192.0.2.165/24 to a destination server with the IP address of 192.0.2.166.

```
cluster1::network routing-groups> create -vserver node1 -routing-group  
192.0.2.166 -subnet 192.0.2.165/24 -role data -metric 20
```

### See Also

---

network routing-groups route create

---

## network routing-groups delete

Delete a routing group

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

### Description

The `network routing-groups delete` command deletes a specified group of static routes.

Note:

Before you run this command, you must delete any logical interfaces that are using this routing group. Use the `network interface delete` command to delete any logical interfaces using this group.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies the node or Vserver from which the routing group will be deleted

**-routing-group** <text> - Routing Group

Specifies the name of the routing group that you want to delete.

### Examples

The following example deletes a routing group from the Vserver node1 with an IP address of 192.0.2.165/24.

```
cluster1::network routing-groups> delete -vserver node1 -routing-group  
192.0.2.165/24
```

### See Also

`network interface delete`

---

## network routing-groups show

Display routing groups

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

### Description

The `network routing-groups show` command displays a group of static routes. You can view routes originating from specified servers, and routes with specified names, roles, and number of hops.

### Parameters

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

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

| [-**instance** ] }

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

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

Use this parameter to display the routing groups within the specified vservers.

[-**routing-group** <text>] - Routing Group

Use this parameter to display the specified routing group.

[-**subnet** <IpAddress/Mask>] - Address/Mask

Use this parameter to display the routing groups within the specified subnet. The format for this value is: address, slash ("/"), mask. The example below has `192.0.2.165/24` as a valid value for the `-subnet` parameter.

[-**role** {cluster|data|node-mgmt|intercluster|cluster-mgmt}] - Role

Use this parameter to display the routing groups with the specified role.

[-**metric** <integer>] - Metric

Use this parameter to display the routing groups with the specified metric.

---

**[-address-family {ipv4|ipv6|ipv6z}] - Address Family**

Use this parameter to display the routing groups using the specified IP address family. Only IPv4 and IPv6 non-zoned addresses can be used as value for this parameter. IPv6z addresses should not be used.

**Examples**

The following example displays a routing group for data from the virtual server node1.

```
cluster1::> network routing-groups show -role data
Server  Routing      Subnet      Role      Metric
-----  ---
node1   d192.0.2.165/24  192.0.2.165/24  data      20
node2   d192.0.2.166/24  192.0.2.166/24  data      20
2 entries were displayed.
```

---

## network routing-groups route create

Create a static route

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

### Description

The `network routing-groups route create` command creates a static route within a routing group. You can create routes originating from specified Vservers within a specified routing group, routes with specified gateways, and routes with a specified number of hops.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the node or Vserver on which the route is to be created.

**-routing-group** <text> - Routing Group

Use this parameter to specify the name of the routing group within which you want to create the new route.

**-destination** <IpAddress/Mask> - Destination/Mask

Use this parameter to specify the IP address and subnet mask of the route's destination. The format for this value is: address, slash ("/"), mask. The example below has 0.0.0.0/0 as a valid value for the `-destination` parameter.

**-gateway** <IP Address> - Gateway

Use this parameter to specify the IP address of the gateway server leading to the route's destination.

**[-metric** <integer>] - Metric

Use this parameter to specify the hop count for the route you are creating. The default is 20 hops.

### Examples

The following example creates a route within a routing group originating from Vserver node3.

---

```
cluster1::> network routing-groups route create -vserver node3 -routing-group  
d192.0.2.167/24 -destination 0.0.0.0/0 -gateway 10.61.208.1 -metric 10
```

## network routing-groups route delete

Delete a static route

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

### Description

The `network routing-groups route delete` command deletes a static route from a routing group. You can delete routes originating from specified Vservers, and routes within specified routing groups.

### Parameters

**-vserver** <vserver> - Vserver Name

Use this parameter to specify the node or Vserver from which the route will be deleted.

**-routing-group** <text> - Routing Group

Use this parameter to specify the name of the routing group within which you want to delete the route.

**-destination** <IpAddress/Mask> - Destination/Mask

Use this parameter to specify the IP address and subnet mask of the route you want to delete. The format for this value is: address, slash ("/"), mask. For example, 0.0.0.0/0 is a correctly formatted value for the `-destination` parameter.

### Examples

The following example deletes a route within routing group d192.0.2.167/24 originating from Vserver node3.

```
cluster1::> network routing-groups route delete -vserver node3 -routing-group  
d192.0.2.167/24 -destination 0.0.0.0/0
```

## network routing-groups route show

Display static routes



---

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

## Description

The `network routing-groups route show` command displays a group of static routes within one or more routing groups. You can view routes originating from specified servers, routes within specified routing groups, routes with specified gateways, and routes with a specified number of hops.

## Parameters

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

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

| [-**instance** ] }

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

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

Use this parameter to display the routes within the specified vservers.

[-**routing-group** <text>] - Routing Group

Use this parameter to display the routes within the specified routing group.

[-**destination** <IpAddress/Mask>] - Destination/Mask

Use this parameter to display the routes with the specified destination IP address. The format for this value is: address, slash ("/"), mask. The example below has `0.0.0.0/0` as a valid value for the `-destination` parameter.

[-**gateway** <IP Address>] - Gateway

Use this parameter to display the routes with the specified gateway.

[-**metric** <integer>] - Metric

Use this parameter to display the routes with the specified metric.

[-**address-family** {ipv4|ipv6|ipv6z}] - Address Family

Use this parameter to display the routes using the specified address family. Only IPv4 and IPv6 non-zoned addresses can be used for this parameter. IPv6z addresses should not be used.

---

# Examples

The following example displays information about all routing groups.

```
cluster1::> network routing-groups route show
Routing
Server  Group      Destination      Gateway      Metric
-----  -
node1   d192.0.2.165/24
         0.0.0.0/0      10.61.208.1      20
node2   d192.0.2.166/24
         0.0.0.0/0      10.61.208.1      20
2 entries were displayed.
```

---

## qos policy-group create

Create a policy group

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

### Description

The `qos policy-group create` command creates a new policy group. You can use a QoS policy group to control a set of storage objects known as "workloads" - LUNs, volumes, files, or Vservers. Policy groups define measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

After you create a policy group, you use the storage object create command or the storage object modify command to apply the policy group to a storage object.

### Parameters

**-policy-group** <text> - Policy Group Name

Specifies the name of the policy group. Policy group names must be unique and are restricted to 127 alphanumeric characters including underscores "\_" and hyphens "-". Policy group names must start with an alphanumeric character. You use the `qos policy group rename` command to change the policy group name.

**-vserver** <vserver name> - Vserver

Specifies the data Vserver to which this policy group belongs. You can apply this policy group to only the storage objects contained in the specified Vserver. For example, if you want to apply this policy group to a volume, that volume must belong to the specified Vserver. Using this parameter does not apply the policy group's SLOs to the Vserver. You need to use the `vserver modify` command if you want to apply this policy group to the Vserver. If the system has only one Vserver, then the command uses that Vserver by default. QoS policy groups cannot belong to Vservers with Infinite Volumes.

**[-max-throughput** <qos\_tput>] - Maximum Throughput

Specifies the maximum throughput for the policy group. A maximum throughput limit specifies the throughput that the policy group must not exceed. It is specified in terms of IOPS or MB/s, and the range is zero to infinity.

The values entered here are case-insensitive, and the units are base ten. There should be no space between the number and the units. The default value for max-throughput is

---

infinity, which can be specified by the special value "INF". Note there is no default unit - all numbers except zero require explicit specification of the units.

Two reserved keywords, "none" and "INF", are available for the situation that requires removal of a value, and the situation that needs to specify the maximum available value.

Examples of valid throughput specifications are: "100B/s", "10KB/s", "1gb/s", "500MB/s", "1tb/s", and "100iops".

## Examples

```
cluster1::> qos policy-group create p1 -vserver vs1
```

Creates the "p1" policy group which belongs to Vserver "vs1" with default policy values.

```
cluster1::> qos policy-group create p2 -vserver vs1 -max-throughput 500MB/S
```

Creates the "p2" policy group which belongs to Vserver "vs1" with the maximum throughput set to 500 MB/S.

## See Also

`qos policy group rename`

---

## qos policy-group delete

Delete a policy group

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

### Description

The `qos policy-group delete` command deletes a policy group from a cluster. You cannot delete a policy group if it is in use by a storage object, which is also known as a workload.

You can only delete user-defined policy groups. You cannot delete preset policy groups.

### Parameters

**-policy-group** <text> - Policy Group Name

Specifies the name of the policy group that you want to delete.

### Examples

```
cluster1::> qos policy-group delete p1
```

Deletes the "p1" policy group.

---

## qos policy-group modify

Modify a policy group

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

### Description

The `qos policy-group modify` command modifies a user-created policy group.

### Parameters

**-policy-group <text>** - Policy Group Name

Specifies the name of the policy group that you want to modify.

**[-max-throughput <qos\_tput>]** - Maximum Throughput

Specifies the maximum throughput for the policy group. A maximum throughput limit specifies the throughput that the policy group must not exceed. It is specified in terms of IOPS or MB/s, and the range is zero to infinity.

The values entered here are case-insensitive, and the units are base ten. There should be no space between the number and the units. The default value for max-throughput is infinity, which can be specified by the special value "INF". Note there is no default unit - all numbers except zero require explicit specification of the units.

Two reserved keywords, "none" and "INF", are available for the situation that requires removal of a value, and the situation that needs to specify the maximum available value.

Examples of valid throughput specifications are: "100B/s", "10KB/s", "1gb/s", "500MB/s", "1tb/s", and "100iops".

### Examples

```
cluster1::> qos policy-group modify pl -max-throughput 10IOPS
```

Modifies the "p1" policy group and sets its max throughput value to 10 IOPS.

---

## gos policy-group rename

Rename a policy group

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

### Description

The `gos policy-group rename` command changes the name of an existing policy group.

### Parameters

**-policy-group** <text> - Policy Group Name

Specifies the existing name of the policy group that you want to rename.

**-new-name** <text> - New Policy Group Name

Specifies the new name of the policy group. Policy group names must be unique and are restricted to 127 alphanumeric characters including underscores "\_" and hyphens "-". Policy group names must start with an alphanumeric character.

### Examples

```
cluster1::> gos policy-group rename -policy-group p1 -new-name p1_new
```

Renames the policy group from "p1" to "p1\_new".

---

## qos policy-group show

Display a list of policy groups

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

### Description

The `qos policy-group show` command shows the current settings of the policy groups on a cluster. You can display a list of the policy groups and you can view detailed information about a specific policy group.

### Parameters

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

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

| [-**instance** ] }

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

[-**policy-group** <text>] - Policy Group Name

Selects the policy groups that match this parameter value

Policy groups define measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

[-**vserver** <vserver name>] - Vserver

Selects the policy groups that match this parameter value

[-**uuid** <UUID>] - Uuid

Selects the policy groups that match this parameter value

[-**class** {preset|user-defined|system-defined}] - Policy Group Class

Selects the policy groups that match this parameter value

[-**pgid** <integer>] - Policy Group ID

Selects the policy groups that match this parameter value



---

This uniquely identifies the policy group

**[-max-throughput <qos\_tput>]** - Maximum Throughput

Selects the policy groups that match this parameter value

A maximum throughput limit specifies the throughput (in IOPS or MB/s) that the policy group must not exceed.

**[-num-workloads <integer>]** - Number of Workloads

Selects the policy groups that match this parameter value.

**[-throughput-policy <text>]** - Throughput Policy

Selects the policy groups that match this parameter value. You can specify the throughput range in terms of IOPS or data rate. For example, 0-INF, 0-400IOPS, 0-200KB/s, 0-400MB/s.

## Examples

```
cluster11::> qos policy-group show
Name          Vserver      Class          Wklds  Throughput
-----
pg1            vs4          user-defined   0      0-200IOPS
pg2            vs0          user-defined   0      0-500IOPS
pg5            vs0          user-defined   0      0-300IOPS
pg6            vs0          user-defined   0      0-INF
4 entries were displayed.
```

The example above displays all policy groups on the cluster.

---

## qos statistics characteristics show

Display QoS policy group characterization

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

### Description

The `qos statistics characteristics show` command displays data that characterizes the behavior of QoS policy groups.

The command displays the following data:

- The QoS policy group name (Policy Group)
- Input/output operations performed per second (IOPS)
- Throughput achieved in kilobytes per second (KB/s) or megabytes per second (MB/s) as appropriate (Throughput)
- Request size in bytes (B) (Request size)
- Read percentage from total I/O (Read)
- Concurrency, which indicates the number of concurrent users generating the I/O traffic (Concurrency)

The results displayed per iteration are sorted by IOPS. Each iteration starts with a row that displays the total IOPS used across all QoS policy groups. Other columns in this row are either totals or averages.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the policy groups that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS policy groups to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

### Examples

```
cluster1::> qos statistics characteristics show -iterations 100 -rows 4
Policy Group      IOPS      Throughput      Request size      Read      Concurrency
-----
-total-          31      304.00KB/s      10041B      0%      16
_System-Best-Effort 15      0KB/s      0B      0%      0
vol1             11      44.00KB/s      4096B      0%      40
vol2             4       256.00KB/s      65536B      0%      14
vslvol0          1       4.00KB/s      4096B      0%      4
-total-          37      808.00KB/s      22361B      2%      3
_System-Best-Effort 15      0KB/s      0B      0%      0
vol2             12      768.00KB/s      65536B      0%      9
vslvol0          8       32.00KB/s      4096B      12%      1
vol1             2       8.00KB/s      4096B      0%      1
```

The example above displays the characteristics of the 4 QoS policy groups with the highest IOPS values and refreshes the display 100 times before terminating.

---

## qos statistics latency show

Display latency breakdown data per QoS policy group

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

### Description

The `qos statistics latency show` command displays the average latencies for QoS policy groups across the various Data ONTAP subsystems.

The command displays the following data:

- The QoS policy group name (Policy Group)
- Total latency observed per I/O operation (Latency)
- Latency observed per I/O operation in the Network subsystem (Network)
- Latency observed per I/O operation across the internally connected nodes in a Cluster (Cluster)
- Latency observed per I/O operation in the Data management subsystem (Data)
- Latency observed per I/O operation in the Storage subsystem (Disk)
- Latency observed per I/O operation in the QoS subsystem (QoS)

The results displayed per iteration are sorted by the Latency field. Each iteration starts with a row that displays the average latency, in microseconds (us) or milliseconds (ms), observed across all QoS policy groups.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the policy groups that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS policy groups to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

## Examples

```
cluster1::> qos statistics latency show -iterations 100 -rows 3
Policy Group      Latency      Network      Cluster      Data      Disk      QoS
-----
-total-0ms      110.35ms     110.02ms     0ms          327.00us   0ms
vslvol00ms      167.82ms     167.22ms     0ms          603.00us   0ms
voll0ms         117.76ms     117.56ms     0ms          191.00us   0ms
vol20ms         44.24ms      44.05ms      0ms          190.00us   0ms
-total-0ms      38.89ms      38.63ms      0ms          256.00us   0ms
vol20ms         64.47ms      64.20ms      0ms          266.00us   0ms
voll0ms         27.28ms      27.03ms      0ms          253.00us   0ms
vslvol00ms      23.72ms      23.47ms      0ms          249.00us   0ms
-total-0ms      409.81ms     409.65ms     0ms          169.00us   0ms
voll0ms         816.92ms     816.80ms     0ms          120.00us   0ms
vol20ms         407.88ms     407.66ms     0ms          219.00us   0ms
vslvol00ms      3.68ms       3.49ms       0ms          193.00us   0ms
-total-0ms      1169.00us    107.00us     0ms          1062.00us  0ms
vol20ms         1169.00us    107.00us     0ms          1062.00us  0ms
```

The example above displays latencies for the 3 QoS policy groups with the highest latencies and refreshes the display 100 times before terminating.

---

## qos statistics performance show

Display system performance data per QoS policy group

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

### Description

The `qos statistics performance show` command shows the current system performance levels that QoS policy groups are achieving.

The command displays the following data:

- The QoS policy group name (Policy Group)
- Input/output operations performed per second (IOPS)
- Throughput in kilobytes per second (KB/s) or megabytes per second (MB/s) as appropriate (Throughput)
- Latency observed per request in microseconds (us) or milliseconds (ms) as appropriate (Latency)

The results displayed per iteration are sorted by IOPS. Each iteration starts with a row that displays the total IOPS used across all QoS policy groups. Other columns in this row are either totals or averages.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the policy groups that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS policy groups to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

---

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

## Examples

```
cluster1:>> qos statistics performance show -iterations 100 -rows 4
Policy Group      IOPS      Throughput      Latency
-----
-total-          79      1296.00KB/s      337.41ms
_System-Best-Effort 25          0KB/s           0ms
vol1             24      96.00KB/s       193.72ms
vol2             18     1152.00KB/s      750.98ms
vslvol0          12      48.00KB/s       707.38ms
-total-         109      1.99MB/s       133.27ms
_System-Best-Effort 35          0KB/s           0ms
vol2             29      1.81MB/s       249.27ms
vslvol0          24      96.00KB/s       48.32ms
vol1             21      84.00KB/s       292.30ms
```

The example above displays the system performance for the 4 QoS policy groups with the highest IOPS and it refreshes the display 100 times before terminating.

---

## qos statistics resource cpu show

Display CPU resource utilization data per QoS policy group

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

### Description

The `qos statistics resource cpu show` command displays the CPU utilization for QoS policy groups per node.

The command displays the following data:

- The QoS policy group name (Policy Group)
- CPU utilization observed in percentage (CPU)

The results displayed per iteration are sorted by total CPU utilization. Each iteration starts with a row that displays the total CPU utilization across all QoS policy groups.

### Parameters

**-node** {<nodename>|local} - Node

Selects the policy groups that match this parameter value.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS policy groups to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

### Examples

```
-rows 3 cluster1:> qos statistics resource cpu show -node nodeA -iterations 100
Policy Group          CPU
```



---

```
-----
-total- (100%)      9%
fast                1%
slow                2%
medium              5%
-total- (100%)      8%
slow                1%
fast                3%
medium              3%
```

The example above displays the total CPU utilization for the 3 QoS policy groups with the highest CPU utilization and it refreshes the display 100 times before terminating.

---

## qos statistics resource disk show

Display disk resource utilization data per QoS policy group

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

### Description

The `qos statistics resource disk show` command displays the disk utilization for QoS policy groups per node. The disk utilization shows the percentage of time spent on the disk during read and write operations. The command displays disk utilization for system-defined policy groups; however, their disk utilization is not included in the total utilization.

The command displays the following data:

- The QoS policy group name (Policy Group)
- Disk utilization (Disk)
- The number of data disks utilized (No. of Disks)

The results displayed are sorted by total disk utilization. Each iteration starts with a row that displays the total disk utilization across all QoS policy groups.

### Parameters

**-node** {<nodename>|local} - Node

Selects the policy groups that match this parameter value.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS policy groups to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

---

# Examples

```
cluster1::> qos statistics resource disk show -node nodeA -iterations 100
-rows 3
Policy Group      Disk  No. of Disks
-----
-total-          40%      27
pg1              22%       5
slow             10%      10
fast             8%       12
_System_Default  7%       20
-total-          42%      27
pg1              22%       5
slow             12%      10
fast             8%       12
_System_Default  7%       20
```

The example above displays the total disk utilization for the 3 QoS policy groups with the highest disk utilization and it refreshes the display 100 times before terminating.

---

## qos statistics workload characteristics show

Display QoS workload characterization

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

### Description

The `qos statistics workload characteristics show` command displays data that characterizes the behavior of QoS workloads.

The command displays the following data:

- The QoS workload name (Workload)
- The QoS workload ID (ID)
- Input/output operations performed per second (IOPS)
- Throughput achieved in kilobytes per second (KB/s) or megabytes per second (MB/s) as appropriate (Throughput)
- Request size in bytes (B) (Request size)
- Read percentage from total IOPS (Read)
- Concurrency, which indicates the number of concurrent users generating the I/O traffic (Concurrency)

The results displayed per iteration are sorted by IOPS. Each iteration starts with a row that displays the total IOPS used across all QoS workloads. Other columns in this row are either totals or averages.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the QOS workloads that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS workloads to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

### Examples

```
cluster1:> qos statistics workload characteristics show -iterations 100 -
rows 4
Workload      ID      IOPS      Throughput      Request size      Read
Concurrency
-----
-total-      -      68      176.00KB/s      2650B      7%
8
vslvol0-wid102 102      24      96.00KB/s      4096B      20%
13
_Scan_Besteff.. 101      23      0KB/s      0B      0%
0
vol_1-wid103    103      20      80.00KB/s      4096B      0%
12
vol_2-wid104    104      1      0KB/s      0B      0%
0
-total-      -      157     528.00KB/s      3443B      3%
4
vol_2-wid104    104      48      192.00KB/s      4096B      0%
9
vol_1-wid103    103      43      172.00KB/s      4096B      0%
0
vslvol0-wid102 102      41      164.00KB/s      4096B      14%
6
_Scan_Besteff.. 101      25      0KB/s      0B      0%
0
-total-      -      274     1016.00KB/s     3797B      2%
2
vslvol0-wid102 102      85      340.00KB/s      4096B      8%
4
vol_2-wid104    104      85      340.00KB/s      4096B      0%
1
vol_1-wid103    103      84      336.00KB/s      4096B      0%
3
_Scan_Besteff.. 101      20      0KB/s      0B      0%
0
```

The example above displays characteristics for the 4 QoS workloads with the highest IOPS and it refreshes the display 100 times before terminating.

---

## qos statistics workload latency show

Display latency breakdown data per QoS workload

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

### Description

The `qos statistics workload latency show` command displays the average latencies for QoS workloads on Data ONTAP subsystems.

The command displays the following data:

- The QoS workload name (Workload)
- The QoS workload ID (ID)
- Total latency observed per I/O operation (Latency)
- Latency observed per I/O operation in the Network subsystem (Network)
- Latency observed per I/O operation across the internally connected nodes in a Cluster (Cluster)
- Latency observed per I/O operation in the Data management subsystem (Data)
- Latency observed per I/O operation in the Storage subsystem (Disk)
- Latency observed per I/O operation in the QoS subsystem (QoS)

The results displayed per iteration are sorted by the total latency field. Each iteration starts with a row that displays the average latency, in microseconds (us) or milliseconds (ms) observed across all QoS workloads.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the QOS workloads that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times that the command refreshes the display with updated data before terminating. If you do not specify this parameter, the command continues to run until you interrupt it by pressing Ctrl-C.

---

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS workloads to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

## Examples

```
cluster1::> qos statistics workload latency show -iterations 100 -rows 3
Workload      ID      Latency      Network      Cluster      Data      Disk      QoS
-----
-total-      111      110.35ms      110.02ms      0ms      327.00us      0ms      0ms
vslvo10      1234      167.82ms      167.22ms      0ms      603.00us      0ms      0ms
vol1          999      117.76ms      117.56ms      0ms      191.00us      0ms      0ms
vol2          999      44.24ms      44.05ms      0ms      190.00us      0ms      0ms
-total-      -      38.89ms      38.63ms      0ms      256.00us      0ms      0ms
vol2          999      64.47ms      64.20ms      0ms      266.00us      0ms      0ms
vol1          1234      27.28ms      27.03ms      0ms      253.00us      0ms      0ms
vslvo10      111      23.72ms      23.47ms      0ms      249.00us      0ms      0ms
-total-      -      409.81ms      409.65ms      0ms      169.00us      0ms      0ms
vol1          1234      816.92ms      816.80ms      0ms      120.00us      0ms      0ms
vol2          999      407.88ms      407.66ms      0ms      219.00us      0ms      0ms
vslvo10      111      3.68ms      3.49ms      0ms      193.00us      0ms      0ms
```

The example above displays latencies for the 3 QoS workloads with the highest latencies and it refreshes the display 100 times before terminating.

---

## qos statistics workload performance show

Display system performance data per QoS workload

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

### Description

The `qos statistics workload performance show` command shows the current system performance that each QoS workload is achieving.

The command displays the following data:

- The QoS workload name (Workload)
- The QoS workload ID (ID)
- Input/output operations performed per second (IOPS)
- Throughput in kilobytes per second (KB/s) or megabytes per second (MB/s) as appropriate (Throughput)
- Latency observed per request in microseconds (us) or milliseconds (ms) as appropriate (Latency)

The results displayed per iteration are sorted by IOPS. Each iteration starts with a row that displays the total IOPS used across all QoS workloads. Other columns in this row are either totals or averages.

### Parameters

**[-node {<nodename>|local}]** - Node

Selects the QOS workloads that match this parameter value. If you do not specify this parameter, the command displays data for the entire cluster.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS workloads to display. The default setting is 10. The allowed range of values is 1 to 20.



---

## **[-refresh-display {true|false}] - Toggle Screen Refresh Between Each Iteration**

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

## **Examples**

```
cluster1::> qos statistics workload performance show -iterations 100 -rows 4
Workload      ID      IOPS      Throughput      Latency
-----
-total-      -      97      1.90MB/s      216.87ms
_Scan_Besteff.. 101      31      0KB/s      0ms
vol_2-widl04    104      28      1.75MB/s      412.78ms
vol_1-widl03    103      25      100.00KB/s      169.16ms
vslvol0-widl02  102      13      52.00KB/s      403.78ms
-total-      -      98      1276.00KB/s      89.98ms
_Scan_Besteff.. 101      34      0KB/s      0ms
vslvol0-widl02  102      28      112.00KB/s      80.70ms
vol_1-widl03    103      19      76.00KB/s      114.72ms
vol_2-widl04    104      17      1088.00KB/s      257.60ms
-total-      -      78      1152.00KB/s      225.22ms
_Scan_Besteff.. 101      30      0KB/s      0ms
vol_1-widl03    103      17      68.00KB/s      452.27ms
vol_2-widl04    104      16      1024.00KB/s      419.93ms
vslvol0-widl02  102      15      60.00KB/s      210.63ms
```

The example above displays the system performance for the 4 QoS workloads with the highest IOPS and it refreshes the display 100 times before terminating.

---

## qos statistics workload resource cpu show

Display CPU resource utilization data per QoS workload

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

### Description

The `qos statistics workload resource cpu show` command displays the CPU utilization for QoS workloads per node.

The command displays the following data:

- The QoS workload name (Workload)
- The QoS workload ID (ID)
- CPU utilization observed in percentage (CPU)

The results displayed per iteration are sorted by total CPU utilization. Each iteration starts with a row that displays the total CPU utilization across all QoS workloads.

### Parameters

**-node** {<nodename>|local} - Node

Selects the QOS workloads that match this parameter value.

**[-iterations <integer>]** - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows <integer>]** - Number of Rows in the Output

Specifies the number of busiest QoS workloads to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display {true|false}]** - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

### Examples

---

```

cluster1::> qos statistics workload resource cpu show -node nodeA -iterations
100 -rows 3
Workload      ID      CPU
-----
--total- (100%) -      9%
vs0-wid-102    102     5%
file-bigvmdk-.. 121     2%
vs2_vol0-wid-.. 212     2%
--total- (100%) -      8%
vs0-wid-101    102     5%
file-bigvmdk-.. 121     2%
vs2_vol0-wid-.. 212     1%

```

The example above displays total CPU utilization for the 3 QoS workloads with the highest CPU utilization and it refreshes the display 100 times before terminating.

---

## qos statistics workload resource disk show

Display disk resource utilization data per QoS workload

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

### Description

The `qos statistics workload resource disk show` command displays the disk utilization for QoS workloads per node. The disk utilization shows the percentage of time spent on the disk during read and write operations. The command displays disk utilization for system-defined workloads; however, their disk utilization is not included in the total utilization.

The command displays the following data:

- The QoS workload name (Workload)
- The QoS workload ID (ID)
- Disk utilization (Disk)
- The number of data disks utilized (No. of Disks)

The results displayed are sorted by total disk utilization. Each iteration starts with a row that displays the total disk utilization across all QoS workloads.

### Parameters

**-node** {<nodename>|local} - Node

Selects the QOS workloads that match this parameter value.

**[-iterations** <integer>] - Number of Iterations

Specifies the number of times the display is refreshed before terminating. If you do not specify this parameter, the command iterates until interrupted by Ctrl-C.

**[-rows** <integer>] - Number of Rows in the Output

Specifies the number of busiest QoS workloads to display. The default setting is 10. The allowed range of values is 1 to 20.

**[-refresh-display** {true|false}] - Toggle Screen Refresh Between Each Iteration

Specifies the display style. If true, the command clears the display after each data iteration. If false, the command displays each data iteration below the previous one. The default is false.

Examples

```
iterations 100 -rows 3
cluster1:> qos statistics workload resource disk show -node nodeB -
Workload      ID      Disk      No. of Disks
-----
-total- (100%) -      30%      4
_RAID         -      20%      4
vs0-wid101    101    12%      2
file-l-wid121 121    10%      1
vol0-wid1002  1002    8%       1
_WAFL        -       7%       3
-total- (100%) -      30%      4
vs0-wid101    101    12%      2
file-l-wid121 121    10%      1
_RAID         -      10%      4
vol0-wid1002  1002    8%       1
_WAFL        -       7%       3
```

The example above displays total disk utilization for the 3 QoS workloads with the highest disk utilization and it refreshes the display 100 times before terminating.

---

## security snmpusers

Show SNMP users

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

### Description

The `security snmpusers` displays the following information about SNMP users:

- User name
- Authentication method
- Hexadecimal engine ID
- Authentication protocol
- Privacy protocol
- Security group

### Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays information only about the SNMP user or users that belong to the specified Vserver.

[-username <text>] - User Name

If this parameter is specified, the command displays information only about the SNMP user with the specified user name.

[-authmethod <text>] - Authentication Method

If this parameter is specified, the command displays information only about the SNMP user or users that use the specified authentication method. Possible values include the following:

- community-SNMP community strings
- usm-SNMP user security model

**[-engineid <Hex String>]** - Engine Id

If this parameter is specified, the command displays information only about the SNMP user or users that use the specified engine ID, specified in hexadecimal format.

**[-authprotocol <text>]** - Authentication Protocol

If this parameter is specified, the command displays information only about the SNMP user or users that use the specified authentication protocol.

**[-privprotocol <text>]** - Privacy Protocol

If this parameter is specified, the command displays information only about the SNMP user or users that use the specified privacy protocol.

**[-securitygroup <text>]** - Security Group

If this parameter is specified, the command displays information only about the SNMP user or users that belong to the specified security group.

## Examples

The following example displays information about all SNMP users:

```
cluster1::> security snmpusers
```

Vserver	UserName	AuthMethod	EngineId	Protocols Auth Priv Group	Security
cluster1	comm1	community	8000031504312d38302d313233343536	- - -	readwrite
cluster1	private	community	8000031504312d38302d313233343536	- - -	readwrite
vs1	snmpuser1	community	8000031504312d38302d31323334353632	- - -	readwrite
vs1	snmpuser2	usm	8000031504312d38302d31323334353632	- - -	readwrite

---

## security audit modify

Set administrative audit logging settings

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

### Description

The `security audit modify` command modifies the following audit-logging settings for the management interface:

- Whether set requests for the CLI are audited
- Whether set requests for the Web (HTTP) interface are audited
- Whether set requests for the Data ONTAP API (ONTAPI) are audited
- Whether get requests for the CLI are audited
- Whether get requests for the Web (HTTP) interface are audited
- Whether get requests for the Data ONTAP API (ONTAPI) are audited

### Parameters

**[-cliset {on|off}]** - Enable auditing of CLI set operations

This specifies whether set requests for the CLI are audited. The default setting is `on`.

**[-httpset {on|off}]** - Enable auditing of HTTP set operations

This specifies whether set requests for the Web (HTTP) interface are audited. The default setting is `on`.

**[-ontapiset {on|off}]** - Enable auditing of Data ONTAP API set operations

This specifies whether set requests for the Data ONTAP API (ONTAPI) interface are audited. The default setting is `on`.

**[-cliget {on|off}]** - Enable auditing of CLI get operations

This specifies whether get requests for the CLI are audited. The default setting is `off`.

**[-httpget {on|off}]** - Enable auditing of HTTP get operations

This specifies whether get requests for the Web (HTTP) interface are audited. The default setting is `off`.



---

**[-ontapiget {on|off}]** - Enable auditing of Data ONTAP API get operations

This specifies whether get requests for the Data ONTAP API (ONTAPI) interface are audited. The default setting is `off`.

## Examples

The following example turns off auditing of get and set requests for the Web interface:

```
cluster1::> security audit modify -httpset off -httpget off
```

## security audit show

Show administrative audit logging settings

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

## Description

The `security audit show` command displays the following audit-logging settings for the management interface:

- Whether set requests for the CLI are audited
- Whether set requests for the Web (HTTP) interface are audited
- Whether set requests for the Data ONTAP API (ONTAPI) are audited
- Whether get requests for the CLI are audited
- Whether get requests for the Web (HTTP) interface are audited
- Whether get requests for the Data ONTAP API (ONTAPI) are audited

## Parameters

None

## Examples

The following example displays the audit-logging settings for the management interface:

```
cluster1::> security audit show
Auditing State for
Set Requests:
-----
CLI:         off
HTTP:        off
ONTAPI:      on

Auditing State for
Get Requests:
-----
CLI:         off
HTTP:        off
ONTAPI:      on
```

---

## security certificate create

Create and Install a Self-Signed Digital Certificate

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

### Description

This command creates and installs a self-signed digital certificate, which can be used either for server authentication or for signing other certificates by acting as certificate authority (CA). The certificate function is selected by the `-type` field. Self-signed digital certificates are not as secure as certificates signed by a certificate authority (CA). Therefore, they are not recommended in a production environment.

### Parameters

**-vserver** <vserver name> - Name of Vserver

This specifies the name of the Vserver on which the certificate will exist.

**-common-name** <FQDN or Custom Common Name> - FQDN or Custom Common Name

This specifies the desired certificate name as a fully qualified domain name (FQDN) or custom common name or the name of a person.

**-type** <type of certificate> - Type of Certificate

This specifies the type of certificate, either server or root-ca. The server type creates and installs a self-signed digital certificate to be used for server authentication, whereas root-ca creates and installs a self-signed digital certificate to sign other certificates by acting as certificate authority (CA).

**-size** <size of requested certificate in bits> - Size of Requested Certificate in Bits

This specifies the number of bits in the private key. The larger the value, the more secure is the key. The default is 2048. Possible values include 512, 1024, 1536 and 2048.

**-country** <text> - Country Name

This specifies the country where the Vserver resides. The country name is a two-letter code. The default is US. Here is the list of country codes: Country Codes

**-state** <text> - State or Province Name

---

This specifies the state or province where the Vserver resides.

**-locality** <text> - Locality Name

This specifies the locality where the Vserver resides. For example, the name of a city.

**-organization** <text> - Organization Name

This specifies the organization where the Vserver resides. For example, the name of a company.

**-unit** <text> - Organization Unit

This specifies the unit where the Vserver resides. For example, the name of a section or a department within a company.

**-email-addr** <mail address> - Contact Administrator's Email Address

This specifies the email address of the contact administrator for the Vserver.

**-expire-days** <integer> - Number of Days until Expiration

This specifies the number of days until the certificate expires. The default is 365 days. Possible values are between 1 and 36510.

**-hash-function** <hashing function> - Hashing Function

This specifies the cryptographic hashing function for signing the certificate. The default is SHA256. Possible values include SHA1, SHA256 and MD5.

## Examples

This example creates a server type, self-signed digital certificate for a Vserver named vs0 at a company whose custom common name is www.example.com and whose Vserver name is vs0.

```
cluster1::> security certificate create -vserver vs0 -common-name www.example.com  
-type server
```

This example creates a root-ca type, self-signed digital certificate with a 2048-bit private key generated by the SHA256 hashing function that will expire in 365 days for a Vserver named vs0 for use by the Software group in IT at a company whose custom common name is www.example.com, located in Sunnyvale, California, USA. The email address of the contact administrator who manages the Vserver is web@example.com.

```
cluster1::> security certificate create -vserver vs0 -common-name www.example.com  
-type root-ca -size 2048 -country US -state California -locality Sunnyvale -  
organization IT -unit Software -email-addr web@example.com -expire-days 365 -  
hash-function SHA256
```

---

## security certificate delete

Delete an Installed Digital Certificate

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

### Description

This command deletes an installed digital security certificate.

### Parameters

**-vserver** <vserver name> - Name of Vserver

This specifies the Vserver that contains the certificate.

**-common-name** <FQDN or Custom Common Name> - FQDN or Custom Common Name

This specifies a fully qualified domain name (FQDN) or custom common name or the name of a person.

**[-serial <text>]** - Serial Number of Certificate

This specifies the certificate serial number. The default value is "".

**-ca** <text> - Certificate Authority

This specifies the certificate authority (CA).

**-type** <type of certificate> - Type of Certificate

This specifies the certificate type. See Also: `security certificate create`

### Examples

This example deletes the security certificate for a Vserver named vs0 in a company named www.example.com.

```
cluster1::> security certificate delete -vserver vs0 -common-name www.example.com  
-ca "Verisign Inc" -type server
```

This example deletes a root-ca type digital certificate for a Vserver named vs0 in a company named www.example.com with serial number 4F57D3D1.

```
cluster1::> security certificate delete -vserver vs0 -common-name www.example.com  
-ca www.example.com -type root-ca -serial 4F57D3D1
```

---

## See Also

security certificate create

---

## security certificate generate-csr

Generate a Digital Certificate Signing Request

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

### Description

This command generates a digital certificate signing request and displays it on the console. A certificate signing request (CSR or certification request) is a message sent securely to a certificate authority (CA) via any electronic media, to apply for a digital identity certificate.

### Parameters

**-common-name** <FQDN or Custom Common Name> - FQDN or Custom Common Name

This specifies the desired certificate name as a fully qualified domain name (FQDN) or custom common name or the name of a person.

**[-size** <size of requested certificate in bits>] - Size of Requested Certificate in Bits

This specifies the number of bits in the private key. The higher the value, the more secure is the key. The default is 2048. Possible values include 512, 1024, 1536 and 2048.

**[-country** <text>] - Country Name

This specifies the country where the Vserver resides. The country name is a two-letter code. The default is US. Here is the list of country codes: Country Codes

**[-state** <text>] - State or Province Name

This specifies the state or province where the Vserver resides.

**[-locality** <text>] - Locality Name

This specifies the locality where the Vserver resides. For example, the name of a city.

**[-organization** <text>] - Organization Name

This specifies the organization where the Vserver resides. For example, the name of a company.

**[-unit** <text>] - Organization Unit

---

This specifies the unit where the Vserver resides. For example, the name of a section or a department within a company.

**[-email-addr <mail address>]** - Contact Administrator's Email Address

This specifies the email address of the contact administrator for the Vserver.

**[-hash-function <hashing function>]** - Hashing Function

This specifies the cryptographic hashing function for signing the certificate. The default is SHA256. Possible values include SHA1, SHA256 and MD5.

## Examples

This example creates a certificate-signing request with a 2048-bit private key generated by the SHA256 hashing function for use by the Software group in IT at a company whose custom common name is www.example.com, located in Sunnyvale, California, USA. The email address of the contact administrator who manages the Vserver is web@example.com.

```
cluster1::> security certificate generate-csr -common-name www.example.com
-size 2048 -country US -state California -locality Sunnyvale -organization IT -
unit Software
-email-addr web@example.com -hash-function SHA256
```

```
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQODEwtleGFtcGx1LnNvbTETMAkGA1UEBhMCVVMx
CTAHBgNVBAQTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCCTAHBgNVBAStADEPMA0G
CSqGS1b3DQEBJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixgImRRGZCR7tVmTYyqPSuTvfVhVtwDjbmXuJ6U3alwoUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGS1b3DQEBECwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHVXloqEOhYECn/NX9h8mbphCom5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

```
Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixgImRRGZCR7tVmTYyqPSuTvfVhVtwDjbm
XuJ6U3alwoUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FkezEuIrQlu
KoMyRYK455wtMk8BrOyJfYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+jlhrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDb0ooWlVvu
xj4aitxVBu6ByVckYU8LbsferNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NctEYxd0Q5
cwBZ5NfZeMBpwQIhAPkOKWQSLadGfsKO077itF+h9FGFNHbtuNtrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.





```

-----BEGIN CERTIFICATE-----
MIIE+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGAlUEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEXhodHRwO18vd3d3LnZhbG1jZXXJ0LmNvbS8xIDAeBgkqhkiG9w0BCQEWew1uZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoxDTI0MDYyOTE3MDYyMFowYzELMAKGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBERWRkeSBHcm9lcCwgSW51JlJExMC8GA1UECXMor28gRGFkZkZkZkQ2xhc3MgMiBDZXJ0-----END CERTIFICATE-----

```

Do you want to continue entering root and/or intermediate certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

```

-----BEGIN CERTIFICATE-----
MIIC5zCCA1ACAQEWdQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGAlUEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEXhodHRwO18vd3d3LnZhbG1jZXXJ0LmNvbS8xIDAeBgkqhkiG9w0BCQEWew1uZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTU5MDYyNjAwMTk1NFowgbsxJDAiBgNVBACTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGAlUEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEXhodHRw-----END CERTIFICATE-----

```

Do you want to continue entering root and/or intermediate certificates {y|n}: n

Note: You should keep a copy of your certificate and private key for future reference.  
If you revert to an earlier release, the certificate and private key are deleted.

**This example installs a certificate of Certificate Authority for client authentication for a Vserver named vs0.**

```
cluster1:> security certificate install -vserver vs0 -type client-ca
```

Please enter Certificate: Press <Enter> when done

```

-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNh1iIsXjOKUgodJfTncJVDANBgkqhkiG9w0BAQUFADCBzjELMAKGA1UEBhMCWkExFTATBgNVBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMjQ2FwZSBub3duMR0wGwYDVQQKEXRUAzGF3dGUgQ29uc3VsdGluZyBjYzYzEoMCMYGA1UECxmFQ2VydGlmawNhdG1vbiBTZXJ2aWNlcyBEaXZpc2lvbjEhMB8GA1UEAxMYVGhhZ3RlIFByZW1pdW0gU2VydMvyIENBMSgwJgYJKoZIhvcNAQkBFhlwcmVtaXVtLXNlcnZlckB0aGF3dGUuY29tMB4XDTk2MDgwMTAwMDAwMFoxDTIxMDEwMTIzNTk1OVowgc4xZzAJBgNVBAYTAlpBMRUwEwYDVQQIEWxXZXN0ZXJueIENhcGUxeEjaQBgNVBACT-----END CERTIFICATE-----

```

Note: You should keep a copy of your certificate and private key for future reference. If you revert or downgrade to an earlier release, you must first delete the certificate and private key.

---

## security certificate show

Display Installed Digital Certificates

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

### Description

This command displays the following information about the digital certificates:

- Vserver
- Serial number of certificate
- FQDN or custom common name or the name of a person
- Type of certificate (*server*, *root-ca*, *client-ca*, *server-chain*)
- Certificate Authority
- Expiration date

To display more details, run the command with the `-instance` parameter. This will add the following information:

- Size in bits of the requested certificate (512, 1024, 1536, 2048)
- Certificate start date
- Public key certificate
- Country name
- State or province name
- Locality name
- Organization name
- Organization unit
- Contact administrator's email address
- Protocol (SSL)
- Hashing function (SHA1, SHA256, MD5)

### Parameters

---

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Name of Vserver

Selects the certificates that match this parameter value.

[-**common-name** <FQDN or Custom Common Name>] - FQDN or Custom Common Name

Selects the certificates that match this parameter value.

[-**serial** <text>] - Serial Number of Certificate

Selects the certificates that match this parameter value.

[-**ca** <text>] - Certificate Authority

Selects the certificates that match this parameter value.

[-**type** <type of certificate>] - Type of Certificate

Selects the certificates that match this parameter value.

[-**size** <size of requested certificate in bits>] - Size of Requested Certificate in Bits

Selects the certificates that match this parameter value.

[-**start** <Date>] - Certificate Start Date

Selects the certificates that match this parameter value.

[-**expiration** <Date>] - Certificate Expiration Date

Selects the certificates that match this parameter value.

[-**public-cert** <certificate>] - Public Key Certificate

Selects the certificates that match this parameter value.

[-**country** <text>] - Country Name

Selects the certificates that match this parameter value.

[-**state** <text>] - State or Province Name

Selects the certificates that match this parameter value.

---

**[-locality <text>]** - Locality Name

Selects the certificates that match this parameter value.

**[-organization <text>]** - Organization Name

Selects the certificates that match this parameter value.

**[-unit <text>]** - Organization Unit

Selects the certificates that match this parameter value.

**[-email-addr <mail address>]** - Contact Administrator's Email Address

Selects the certificates that match this parameter value.

**[-protocol <protocol>]** - Protocol

Selects the certificates that match this parameter value.

**[-hash-function <hashing function>]** - Hashing Function

Selects the certificates that match this parameter value.

## Examples

The examples below display information about digital certificates.

```
cluster1::> security certificate show

Vserver      Serial Number  Common Name  Type
-----
vs0          4F4E4D7B      www.example.com  server
Certificate Authority: www.example.com
Expiration Date: Thu Feb 28 16:08:28 2013

cluster1::*> security certificate show -instance
Vserver: vs0
FQDN or Custom Common Name: www.example.com
Serial Number of Certificate: 4F4E4D7B
Certificate Authority: www.example.com
Type of Certificate: server
Size of Requested Certificate(bits): 2048
Certificate Start Date: Fri Apr 30 14:14:46 2010
Certificate Expiration Date: Sat Apr 30 14:14:46 2011
Public Key Certificate: -----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFAADBGMRQwEgYDVQQDEwtsYWlu
YWJjLmNvb3RlcjEwLWVudC51b3RlcjEwLWVudC51b3RlcjEwLWVudC51b3RlcjEw
VQKKEwAxCCTAHBgNVBAsTADQwLWVudC51b3RlcjEwLWVudC51b3RlcjEwLWVudC51
BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCEwG7dYGe51akE14ecaCdL+LOAxUMA0G
CSqSgIb3DQEBChUAA4IBAQBjLE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZOM1Bhy6Q
+gsE3XEtN07AE4npjIT0eVP0nI9QIJAbP0uPKaCGAVBSBM0M2mOwbfswI7aJoEh
+XuEoNr0G0z+mltnfhgvl1fT6Ms
-----END CERTIFICATE-----

+xxd3LGZYT2worus2
Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (e.g. city): Sunnyvale
Organization Name (e.g. company): example
Organization Unit (e.g. section): IT
Email Address (Contact Name): web@example.com
```

---

Protocol: SSL  
Hashing Function: SHA256

---

## security certificate sign

Sign a Digital Certificate using Self-Signed Root CA

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

### Description

This command signs a digital certificate signing request and generates a certificate using a Self-Signed Root CA certificate in either PEM or PKCS12 format. You can use the `security certificate generate-csr` command to generate a digital certificate signing request.

### Parameters

**-vserver** <vserver name> - Name of Vserver

This specifies the name of the Vserver on which the signed certificate will exist.

**-ca** <text> - Certificate Authority to Sign

This specifies the name of the Certificate Authority that will sign the certificate.

**-ca-serial** <text> - Serial Number of CA Certificate

This specifies the serial number of the Certificate Authority that will sign the certificate.

**[-expire-days** <integer>] - Number of Days until Expiration

This specifies the number of days until the signed certificate expires. The default is 365 days. Possible values are between 1 and 36510.

**[-format** <certificate format>] - Certificate Format

This specifies the format of signed certificate. The default value is PEM. Possible values include PEM and PKCS12.

**[-destination** {(ftp|http)://(hostname|IPv4 Address|'IPv6 Address')}...] - Where to Send File

This specifies the destination to upload the signed certificate. This option can only be used when the format is PKCS12.

**[-hash-function** <hashing function>] - Hashing Function

This specifies the cryptographic hashing function for the self-signed certificate. The default value is SHA256. Possible values include SHA1, SHA256 and MD5.

---

## Examples

This example signs a digital certificate for a Vserver named vs0 using a Certificate Authority certificate that has a ca of www.ca.com and a ca-serial of 4F4EB629 in PEM format using the SHA256 hashing function.

```
cluster1:> security certificate sign -vserver vs0 -ca www.ca.com -ca-serial 4F4EB629 -expire-days 36 -format PEM -hash-function SHA256
```

Please enter Certificate Signing Request(CSR): Press <Enter> when done

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBqMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGAlUEBhMCVVMx
CTAHBqNVBAgTADAJMAcGAlUEBxMAMQkwBwYDVQQKEwAxCtAHBqNVBAStADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixgImRRGZCR7tVmTYyqPSuTvfHvTwdJbmXuj6U3alwoUsb13wfEvQnHVFnci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBEwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHVXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Signed Certificate: :

```
-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIETloskDANBgkqhkiG9w0BAQsFADBDmREwDwYDVQQDEwh2
czAuY2VydbELMAkGAlUEBhMCVVMxCTAHBqNVBAgTADAJMAcGAlUEBxMAMQkwBwYD
VQQKEwAxCtAHBqNVBAStADEPMA0GCSqGSIb3DQEJARYAMB4XDTEyMDMwOTE2MTUx
Ml0xDTYyMDQxNDE2MTUxMl0wYDEUMBIgAlUEAxMLZXXhbXBsZS5jb20xCzAJBgNV
BAYTA1VTMqkwBwYDVQQIEwAxCtAHBqNVBAStADEPMAcGAlUEChMAMQkwBwYDVQQL
EwAxZANBgkqhkiG9w0BCQEWADBCMA0GCSqGSIb3DQEBQUAA0sAMEgCQQDlxWpz
-----END CERTIFICATE-----
```

This example signs and exports a digital certificate to destination ftp://10.98.1.1//u/sam/sign.pfx for a Vserver named vs0 using a Certificate Authority certificate that expires in 36 days and has a ca value of www.ca.com and a ca-serial value of 4F4EB629 in PKCS12 format by the MD5 hashing function.

```
cluster1:> security certificate sign -vserver vs0 -ca www.ca.com -ca-serial 4F4EB629 -expire-days 36 -format PKCS12 -destination ftp://10.98.1.1//u/sam/sign.pfx -hash-function MD5
```

Please enter Certificate Signing Request(CSR): Press <Enter> when done

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBqMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGAlUEBhMCVVMx
CTAHBqNVBAgTADAJMAcGAlUEBxMAMQkwBwYDVQQKEwAxCtAHBqNVBAStADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixgImRRGZCR7tVmTYyqPSuTvfHvTwdJbmXuj6U3alwoUsb13wfEvQnHVFnci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBEwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHVXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Signed Certificate: :

```
-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIETlot8jANBgkqhkiG9w0BAQsFADBDmREwDwYDVQQDEwh2
czAuY2VydbELMAkGAlUEBhMCVVMxCTAHBqNVBAgTADAJMAcGAlUEBxMAMQkwBwYD
VQQKEwAxCtAHBqNVBAStADEPMA0GCSqGSIb3DQEJARYAMB4XDTEyMDMwOTE2MTJw
Nl0xDTYyMDQxNDE2MTUxMl0wYDEUMBIgAlUEAxMLZXXhbXBsZS5jb20xCzAJBgNV
BAYTA1VTMqkwBwYDVQQIEwAxCtAHBqNVBAStADEPMAcGAlUEChMAMQkwBwYDVQQL
EwAxZANBgkqhkiG9w0BCQEWADBCMA0GCSqGSIb3DQEBQUAA0sAMEgCQQDlxWpz
oarXHSyDzy3T5QIxGBGRJ0ActgdjJuqtuAdmnKvKfLSlo4C90
-----END CERTIFICATE-----
```

Please enter Private Key: Press <Enter> when done

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixgImRRGZCR7tVmTYyqPSuTvfHvTwdJb
mXuj6U3alwoUsb13wfEvQnHVFnci2ninsJ8CAwEAAQJAwT2A0+bW3FkzeEuRlQu
koMxRYK455wtMk8BrOyJfHsB20B28eifjJvRwdTOBEav99M7cEzgPv+p5kaZTTM
gQIHAPsp+jlhrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehA1EA+oDb0ooWlVvu
```

---

```
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

```
Please enter a password for pkcs12 file:
Please enter it again:
```

```
Enter User for Destination URI: sam
Enter Password:
```

## See Also

security certificate generate-csr



---

## security certificate ca-issued revoke

Revoke a Digital Certificate

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

### Description

This command revokes a digital certificate signed by a Self-Signed Root CA.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver on which the certificate is stored.

**-serial** <text> - Serial Number of Certificate

This specifies the serial number of the certificate.

**-ca** <text> - Certificate Authority

This specifies the name of the Certificate Authority whose certificate will be revoked.

**-ca-serial** <text> - Serial Number of CA Certificate

This specifies the serial number of Certificate Authority.

**[-common-name** <FQDN or Custom Common Name>] - FQDN or Custom Common Name

This specifies a fully qualified domain name (FQDN) or custom common name or the name of a person. This field is optional if ca-serial is specified.

### Examples

This example revokes a signed digital certificate for a Vserver named vs0 with serial as 4F5A2DF2 for a Certificate Authority certificate that has a ca of www.ca.com and a ca-serial of 4F4EB629.

```
cluster1::> security certificate ca-issued revoke -vserver vs0 -serial 4F5A2DF2 -  
ca www.ca.com -ca-serial 4F4EB629
```

---

## security certificate ca-issued show

Display CA-Issued Digital Certificates

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

### Description

This command displays the following information about the digital certificates issued by the self-signed root-ca:

- Vserver
- Serial number of certificate
- FQDN or custom common name or the name of a person
- Serial number of CA certificate
- Status (*active*, *revoked*)
- Certificate Authority
- Expiration date
- Revocation date

To display more details, run the command with the `-instance` parameter. This will add the following information:

- Country name
- State or province name
- Locality name
- Organization name
- Organization unit
- Contact administrator's email address

### Parameters

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

---

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

| **[-instance ]** }

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

**[-vserver <vserver name>]** - Vserver

Selects the certificates that match this parameter value.

**[-serial <text>]** - Serial Number of Certificate

Selects the certificates that match this parameter value.

**[-ca <text>]** - Certificate Authority

Selects the certificates that match this parameter value.

**[-ca-serial <text>]** - Serial Number of CA Certificate

Selects the certificates that match this parameter value.

**[-common-name <FQDN or Custom Common Name>]** - FQDN or Custom Common Name

Selects the certificates that match this parameter value.

**[-status <status of certificate>]** - Status of Certificate

Selects the certificates that match this parameter value. Possible values include active and revoked.

**[-expiration <Date>]** - Certificate Expiration Date

Selects the certificates that match this parameter value.

**[-revocation <Date>]** - Certificate Revocation Date

Selects the certificates that match this parameter value.

**[-country <text>]** - Country Name (2 letter code)

Selects the certificates that match this parameter value.

**[-state <text>]** - State or Province Name (full name)

Selects the certificates that match this parameter value.

**[-locality <text>]** - Locality Name (e.g. city)

Selects the certificates that match this parameter value.

---

**[-organization <text>]** - Organization Name (e.g. company)

Selects the certificates that match this parameter value.

**[-unit <text>]** - Organization Unit (e.g. section)

Selects the certificates that match this parameter value.

**[-email-addr <mail address>]** - Email Address (Contact Name)

Selects the certificates that match this parameter value.

## Examples

The examples below display information about CA issued digital certificates.

```
cluster1::> security certificate ca-issued show
```

Vserver	Serial Number	Common Name	Serial Number of CA's Certificate	Status
vs0	4F5A2C90	example.com	4F4EB629	active
	Certificate Authority: vs0.cert			
	Expiration Date: Sat Apr 14 16:15:13 2012			
	Revocation Date: -			
vs0	4F5A2DF2	example.com	4F4EB629	revoked
	Certificate Authority: vs0.cert			
	Expiration Date: Sat Apr 14 16:21:06 2012			
	Revocation Date: Fri Mar 09 17:08:30 2012			

2 entries were displayed.

```
cluster1::> security certificate ca-issued show -instance
```

```

Vserver: vs0
Serial Number of Certificate: 4F5A2C90
Certificate Authority: vs0.cert
Serial Number of CA Certificate: 4F4EB629
FQDN or Custom Common Name: example.com
Status of Certificate: active
Certificate Expiration Date: Sat Apr 14 16:15:13 2012
Certificate Revocation Date: -
Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (e.g. city): Sunnyvale
Organization Name (e.g. company): example
Organization Unit (e.g. section): IT
Email Address (Contact Name): web@example.com
```

---

## security login create

Add a login method

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

### Description

The `security login create` command creates a login method for the management utility. A login method consists of a user name, an application (access method), and an authentication method. A user name can be associated with multiple applications. It can optionally include an access-control role name.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver name of the login method.

**-username** <text> - User Name

This specifies the user name of the login method.

**-application** <text> - Application

This specifies the application of the login method. Possible values include console, http, ontapi, rsh, snmp, service-processor, ssh, and telnet.

Setting this parameter to service-processor grants the user access to the Remote LAN Module (RLM) or the Service Processor (SP), if it is available on the system. Because the RLM and the SP support only password authentication, when you set this parameter to service-processor, you must also set the `-authmethod` parameter to password.

Vserver user accounts cannot access the RLM or the SP. Therefore, you cannot use the `-vserver` parameter when you set this parameter to service-processor.

**-authmethod** <text> - Authentication Method

This specifies the authentication method of the login method. Possible values include the following:

- cert - SSL certificate authentication
- community - SNMP community strings
- domain - Active Directory authentication

- 
- nsswitch - LDAP or NIS authentication
  - password - Password
  - publickey - Public-key authentication
  - usm - SNMP user security model. Refer to "security snmpusers" man page for more details.

**-role <text>** - Role Name

This specifies an access-control role name for the login method.

**[-comment <text>]** - Comment Text

This specifies comment text for the user account, for example, "Guest account". The maximum length is 128 characters.

## Examples

The following command creates a login that has the user name monitor, the application ssh, the authentication method password, and the access-control role guest for Vserver vs.

```
cluster1::> security login create -username monitor -application ssh -authmethod password -role guest -vserver vs
```

The following command creates a login that has the user name monitor, the application ontapi, the authentication method password, and the access-control role vsadmin for Vserver vs.

```
cluster1::> security login create -username monitor -application ontapi -authmethod password -role vsadmin -vserver vs
```

The following command creates a login that has the user name monitor, the application ssh, the authentication method publickey, and the access-control role guest for Vserver vs.

```
cluster1::> security login create -username monitor -application ssh -authmethod publickey -role guest -vserver vs
```

The following command creates a login that has the user name monitor, the application http, the authentication method cert, and the access-control role admin for Vserver cluster.

```
cluster1::> security login create -username monitor -application http -authmethod cert -role admin -vserver cluster
```

The following command creates a login that has the user name monitor in DOMAIN1, the application ssh, the authentication method domain, and the access-control role vsadmin for Vserver vs.

---

```
cluster1::> security login create -username DOMAIN1\monitor -application ssh -  
authmethod domain -role vsadmin -vserver vs
```

The following command creates a login that has a login name monitor in the LDAP or NIS server, the application ssh, the authentication method nsswitch, and the access-control role vsadmin for Vserver vs.

```
cluster1::> security login create -username monitor -application ssh -authmethod  
nsswitch -role vsadmin -vserver vs
```

## security login delete

Delete a login method

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

### Description

The `security login delete` command deletes a login method.

### Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver name of the login method.

**-username** <text> - User Name

This specifies the user name of the login method that is to be deleted. A user name can be associated with multiple applications.

**-application** <text> - Application

This specifies the application of the login method. Possible values include console, http, ontapi, rsh, snmp, service-processor, ssh, and telnet.

**-authmethod** <text> - Authentication Method

This specifies the authentication method of the login method. Possible values include the following:

- cert - SSL certificate authentication
- community - SNMP community strings
- domain - Active Directory authentication
- nsswitch - LDAP or NIS authentication

- 
- password - Password
  - publickey - Public-key authentication
  - usm - SNMP user security model

## Examples

The following command deletes a login that has the username guest, the application ssh, and the authentication method password for Vserver vs.

```
cluster1::> security login delete -username guest -application ssh -authmethod password -vserver vs
```

The following command deletes a login that has the username guest, the application ontapi, and the authentication method cert for Vserver vs.

```
cluster1::> security login delete -username guest -application ontapi -authmethod cert -vserver vs
```

## security login lock

Lock a user account with password auth method

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

## Description

The `security login lock` command locks a specified account, preventing it from accessing the management interface.

## Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver to which the user account belongs.

**-username** <text> - Username

This specifies the user name of the account that is to be locked.

## Examples

The following example locks a user account named jdoe which belongs to the Vserver vs1.

```
cluster1::> security login lock -vserver vs1 -username jdoe
```



---

## security login modify

Modify a login method

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

### Description

The `security login modify` command modifies the access-control role name of a login method.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver name of the login method.

**-username** <text> - User Name

This specifies the user name of the login method that is to be modified. A user name can be associated with multiple applications.

**-application** <text> - Application

This specifies the application of the login method. Possible values include console, http, ontapi, rsh, snmp, service-processor, ssh, and telnet.

**-authmethod** <text> - Authentication Method

This specifies the authentication method of the login method. Possible values include the following:

- cert - SSL certificate authentication
- community - SNMP community strings
- domain - Active Directory authentication
- nsswitch - LDAP or NIS authentication
- password - Password
- publickey - Public-key authentication
- usm - SNMP user security model

**[-role <text>]** - Role Name

---

This modifies the access-control role name for the login method.

**[-comment <text>]** - Comment Text

This specifies comment text for the user account, for example, "Guest account". The maximum length is 128 characters.

## Examples

The following command modifies a login method that has the user name guest, the application ontapi, and the authentication method password to use the access-control role guest for Vserver vs.

```
cluster1::> security login modify -username guest -application ontapi -authmethod password -role guest -vserver vs
```

The following command modifies a login method that has the user name guest, the application ssh, and the authentication method publickey to use the access-control role vsadmin for Vserver vs.

```
cluster1::> security login modify -username guest -application ssh -authmethod publickey -role vsadmin -vserver vs
```

## security login password

Modify a password for a user

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

## Description

The `security login password` command resets the password for a specified user. The command prompts you for the user's old and new password.

## Parameters

**-vserver <vserver name>** - Vserver

This optionally specifies the Vserver name of the login method.

**-username <text>** - Username

This optionally specifies the user name whose password is to be changed. If you do not specify a user, the command defaults to the user name admin.

## Examples

---

The following command resets the password for a user named admin for Vserver vs.

```
cluster1::> security login password -username admin -vserver vs
```

## security login show

Show user login methods

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

### Description

The `security login show` command displays the following information about user login methods:

- User name
- Application (console, http, ontapi, rsh, snmp, service-processor, ssh, or telnet)
- Authentication method (community, password, publickey, or usm)
- Role name
- Whether the account is locked

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Selects the login methods that match this parameter value.

[-**username** <text>] - User Name

Selects the login methods that match this parameter value.

[-**application** <text>] - Application

Selects the login methods that match this parameter value. Possible values include console, http, ontapi, rsh, snmp, service-processor, ssh, and telnet.

**[-authmethod <text>]** - Authentication Method

Selects the login methods that match this parameter value. Possible values include the following:

- cert - SSL certificate authentication
- community - SNMP community strings
- domain - Active Directory authentication
- nsswitch - LDAP or NIS authentication
- password - Password
- publickey - Public-key authentication
- usm - SNMP user security model

**[-role <text>]** - Role Name

Selects the login methods that match this parameter value.

**[-acctlocked {yes|no}]** - Account Locked

Selects the login methods that match this parameter value.

**[-comment <text>]** - Comment Text

Selects the login methods that match this parameter value.

## Examples

The example below displays information about all user login methods:

```
cluster1::> security login show
```

Vserver	UserName	Application	Authentication Method	Role Name	Acct Locked
vs	vsadmin	http	password	vsadmin	yes
vs	vsadmin	ontapi	password	vsadmin	yes
vs	vsadmin	ssh	password	vsadmin	yes
cluster1	admin	console	password	admin	no
cluster1	admin	http	password	admin	no
cluster1	admin	rsh	password	admin	no
cluster1	admin	ssh	password	admin	no
cluster1	admin	telnet	password	admin	no

8 entries were displayed.

---

## security login unlock

Unlock a user account with password auth method

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

### Description

The `security login unlock` command unlocks a specified account, enabling it to access the management interface.

### Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver to which the user account belongs.

**-username** <text> - Username

This specifies the user name of the account that is to be unlocked.

### Examples

The following command unlocks a user account named `jdoe` which belongs to the Vserver `vs1`.

```
cluster1::> security login unlock -vserver vs1 -username jdoe
```

## security login domain-tunnel create

Add authentication tunnel Vserver for administrative Vserver

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

### Description

This command establishes an authentication gateway or "tunnel" for authentication of user accounts via Windows Active Directory authentication, so that such accounts can login to administrative Vservers. To use this feature, you need to complete two tasks before using this command. First, create one or more user accounts using the command `security login create` with `-authmethod domain`. The parameter `-username` should be set to a valid user name previously defined in a Windows Domain Controller's

---

Active Directory. Such user names will be in the format <domainname>\<username> where "domainname" is the name of the CIFS domain server. Next, identify or create a Vserver that is configured with CIFS and uses Windows authentication with the Active Directory server mentioned above. This is the Vserver that will be specified with this command. The tunnel Vserver has to be running or this command will return an error. Only one Vserver is allowed to be used as a tunnel. If you attempt to specify more than one Vserver, the system returns an error. If the tunnel Vserver is stopped or destroyed, user authentication requests for administrative Vservers will fail.

## Parameters

**-vserver** <vserver> - Authentication Tunnel Vserver

This parameter specifies a Vserver that has been configured with CIFS and is associated with a Windows Domain Controller's Active Directory authentication. This Vserver will be used as an authentication tunnel for login accounts so that they can be used with administrative Vservers.

## Examples

The following shows example of commands needed to create login user, create a data Vserver, a cifs server and the security login domain-tunnel create command.

```
cluster1::> security login create -vserver cluster1 -username
DOMAIN1\Administrator -application ssh -authmethod domain -role admin
cluster1::> vserver create -vserver vs -rootvolume vol -aggregate
aggr -ns-switch file -rootvolume-security-style mixed
cluster1::> vserver cifs create -vserver vs -cifs-server vscifs -
domain companyname.example.com -ou CN=Computers
cluster1::> security login domain-tunnel create -vserver vs
```

## See Also

security login create   vserver create   vserver cifs create

---

## security login domain-tunnel delete

Delete authentication tunnel Vserver for administrative Vserver

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

### Description

The `security login domain-tunnel delete` command deletes the tunnel established by the `security login domain-tunnel create` command. An error message will be generated if no tunnel exists.

### Parameters

None

### Examples

The following command deletes the tunnel established by `security login domain-tunnel create`.

```
cluster1::> security login domain-tunnel delete
```

### See Also

`security login domain-tunnel create`

---

## security login domain-tunnel modify

Modify authentication tunnel Vserver for administrative Vserver

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

### Description

The `security login domain-tunnel modify` command modifies or replaces the tunnel Vserver. If a tunnel Vserver is not already specified, it sets the current tunnel Vserver with this Vserver, otherwise, it replaces the current tunnel Vserver with the Vserver that you specify. If the tunnel Vserver is changed, authentication requests via previous Vserver will fail. See `security login domain-tunnel create` for more information.

### Parameters

**[-vserver <vserver>]** - Authentication Tunnel Vserver

This parameter specifies a Vserver that has been configured with CIFS and is associated with a Windows Domain Controller's Active Directory authentication. This Vserver will be used as an authentication tunnel for login accounts so that they can be used with administrative Vservers.

### Examples

The following command modifies the tunnel Vserver for administrative Vserver.

```
cluster1::> security login domain-tunnel modify -vserver vs
```

### See Also

`security login domain-tunnel create`



---

## security login domain-tunnel show

Show authentication tunnel Vserver for administrative Vserver

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

### Description

The `security login domain-tunnel show` command shows the tunnel Vserver that was specified by the `security login domain-tunnel create` or `security login domain-tunnel modify` command.

### Parameters

None

### Examples

The example below shows the tunnel Vserver, `vs`, that is currently used as an authentication tunnel. The output informs you that the table is currently empty if tunnel Vserver has not been specified.

```
cluster1::> security login domain-tunnel show
Tunnel Vserver: vs
```

### See Also

`security login domain-tunnel create`   `security login domain-tunnel modify`

---

## security login publickey create

Add a new public key

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

### Description

The `security login publickey create` associates an existing public key with a user account. This command requires that you enter a valid OpenSSH-formatted public key, a user name, index number, and optionally, a comment.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter optionally specifies the Vserver of the user for whom you are adding the public key.

**-username** <text> - Username

This parameter specifies the name of the user for whom you are adding the public key. If you do not specify a user, the user named `admin` is specified by default.

**[-index <integer>]** - Index

This parameter specifies an index number for the public key. Default value is zero if it is the first public key created for the user, otherwise, one greater than the highest existing index.

**-publickey** <certificate> - Public Key

This specifies the OpenSSH public key, which must be enclosed in double quotation marks.

**[-comment <text>]** - Comment

This optionally specifies comment text for the public key. Note that comment text should be enclosed in quotation marks.

### Examples

The following command associates a public key with a user named `tsmith` for Vserver `vs1`. The public key is assigned index number 5 and the comment text is “This is a new key”.

---

```
cluster1::> security login publickey create -vserver vs1 -username tsmith -index
5 -publickey
"ssh-rsa AAAAB3NzaClyc2EAAAABlwAAAEAspH64CYbUsDQCdW22JnK6J
/vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3l6i8AD0Vfbr5T6HZPCixNAIza
FciDy7hgnmdj9eNGedGr/JNrftQbLDlhZybX+72DpQB0tYWBhe6eDJloPLob
ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
-comment "This is a new key"
```

---

## security login publickey delete

Delete a public key

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

### Description

The `security login publickey delete` command deletes a public key for a specific user. To delete a public key, you must specify a user name and index number.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter optionally specifies the Vserver of the user for whom you are adding the public key.

**-username** <text> - Username

This parameter specifies the name of the user for whom you are deleting a public key. If you do not specify a user, the user named `admin` is specified by default.

**-index** <integer> - Index

This parameter specifies an index number for the public key. Default value is zero if it is the first public key created for the user, otherwise, one greater than the highest existing index.

### Examples

The following command deletes the public key for the user named `tsmith` with the index number 5.

```
cluster1::> security login publickey delete -username tsmith -index 5
```

## security login publickey load-from-uri

Load one or more public keys from a URI

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

---

## Description

The `security login publickey load-from-uri` command loads one or more public keys from a Universal Resource Identifier (URI). To load public keys from a URI, you must specify a user name, the URI from which to load them, and optionally, whether you want to overwrite the existing public keys.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter optionally specifies the Vserver for the user associated with the public keys.

**-username** <text> - Username

This parameter specifies the username for the public keys. If you do not specify a username, the username "admin" is used by default.

**-uri** {(ftp|http):||(hostname|IPv4 Address|['IPv6 Address'])...} - URI to load from

This parameter specifies the URI from which the public keys will be loaded.

**-overwrite** {true|false} - Overwrite Entries

This parameter optionally specifies whether you want to overwrite existing public keys. The default value for this parameter is false. If the value is true and you confirm to overwrite, then the existing public keys are overwritten with the new public keys. If you use the value false or do not confirm the overwrite, then newly loaded public keys are appended to the list of existing public keys using the next available index.

## Examples

The following command shows how to load public keys for the user named tsmith from the URI `ftp://ftp.example.com/identity.pub`. This user's existing public keys are not overwritten.

```
cluster1:>> security login publickey load-from-uri -username tsmith  
-uri ftp://ftp.example.com/identity.pub -overwrite false
```

The following command shows how to load public keys for the user named tsmith from the URI `ftp://ftp.example.com/identity.pub`. This user's existing public keys are overwritten if user entered the option 'y' or 'Y'. The user's existing public keys are not overwritten if user entered the option 'n' or 'N' and the newly loaded public keys are appended to the list of existing public keys using the next available index.

```
cluster03:>> security login publickey load-from-uri -username  
tsmith -uri ftp://ftp.example.com/identity.pub -overwrite true -vserver  
vs0
```

```
Enter User:  
Enter Password:
```

---

Warning: You are about to overwrite the existing publickeys for the user  
"tsmith" in Vserver "vs0". Do you want to proceed? {y|n}:

---

## security login publickey modify

Modify a public key

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

### Description

The `security login publickey modify` command modifies a public key and optionally its comment text.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the user associated with the public key.

**-username** <text> - Username

Specifies the username for the public key. If you do not specify a username, the username 'admin' is used by default.

**-index** <integer> - Index

Specifies the index number of the public key. The index number of the public key can be found by using the `security login publickey show` command.

**[-publickey <certificate>]** - Public Key

Specifies the new public key. You must enclose the new public key in double quotation marks.

**[-comment <text>]** - Comment

Specifies the new comment text for the public key.

### Examples

The following command modifies the public key at index number 10 for the user named tsmith of Vserver vs1.

```
cluster1::> security login publickey modify -vserver vs1 -username tsmith -index
10 -publickey
"ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDDD+pFzFgV/2dlowKRFgym9K910H/u
+BVtG1tCtHteHyo8thmaXT
lGLCzaoC/12+XX1YKMRhJ00S9Svo4QQKUXHdCPXFSgr5PnAs39set39ECCLzmduplJnkWtX96pQH/
bg2g3upFcdC6z9
c37uqFtNVPfv8As1Si/9WDQmEJ2mRtJudJeU5GZwZw5ybgTaN1jxDWus9SO2C43F/vmoCKVT529UHt4/
ePcaaHOGT1Q
08+Qmm59uTgcfnpg53zYkpeAQV8RdYtMdWlRr44neh1WZrmW7x5N4nXNvtEzr9cvb9sJyqTX1CkQGfD0db
+7T7y3X7M
```

---

if/qKQY6FsovjvfZD"

## See Also

security login publickey show



---

## security login publickey show

Display public keys

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

### Description

The `security login publickey show` command displays information about public keys.

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Selects the public keys that match this parameter value.

[-**username** <text>] - Username

Selects the public keys that match this parameter value.

[-**index** <integer>] - Index

Selects the public keys that match this parameter value. The default value is zero if it is the first public key created for the user, otherwise, one greater than the highest existing index.

[-**publickey** <certificate>] - Public Key

Selects the public keys that match this parameter value.

[-**fingerprint** <text>] - Hex Fingerprint

Selects the public keys that match this parameter value.

[-**bubblebabble** <text>] - Bubblebabble Fingerprint

---

Selects the public keys that match this parameter value.

**[-comment <text>]** - Comment

Selects the public keys that match this parameter value.

## Examples

The example below displays public key information for the user named tsmith.

```
cluster1::> security login publickey show -username tsmith
UserName: tsmith Index: 5
Public Key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
/vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJloPLob
ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com
Fingerprint:
07:B4:27:52:ce:7f:35:81:5a:f2:07:cf:c1:87:91:97
Bubblebabble fingerprint:
xuzom-nelug-bisih-nihyr-metig-kemal-puhut-somyd-mumuh-zomis-syxex
Comment:
This is a new key
```

---

## security login role create

Add an access control role

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

### Description

The `security login role create` command creates an access-control role. An access-control role consists of a role name and a command or directory to which the role has access. It optionally includes an access level (none, read-only, or all) and a query that applies to the specified command or command directory. After you create an access-control role, you can apply it to a management-utility login account by using the `security login modify` or `security login create` commands.

### Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver name associated with the role.

**-role** <text> - Role Name

This specifies the role that is to be created.

**-cmddirname** <text> - Command / Directory

This specifies the command or command directory to which the role has access. If you want the default setting, use the special string "DEFAULT" as the value.

**[-access <Access>]** - Access Level

This optionally specifies an access level for the role. Possible access level settings are none, read-only, and all. The default setting is `all`.

**[-query <query>]** - Query

This optionally specifies the object that the role is allowed to access. The query object must be applicable to the command or directory name specified by `-cmddirname`. The query object must be enclosed in double quotation marks (""), and it must be a valid field name.

### Examples

---

The following command creates an access-control role named "admin" for the vs1 Vserver. The role has all access to the "volume" command but only within the "aggr0" aggregate.

```
cluster1::> security login role create -role admin -cmddirname volume -query "-  
aggr aggr0" -access all -vserver vs1
```

## See Also

security login modify   security login create

---

## security login role delete

Delete an access control role

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

### Description

The `security login role delete` command deletes an access-control role.

### Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver name associated with the role.

**-role** <text> - Role Name

This specifies the role that is to be deleted.

**-cmddirname** <text> - Command / Directory

This specifies the command or command directory to which the role has access. If you want the default setting, use the special string "DEFAULT" as the value.

### Examples

The following command deletes an access-control role with the role name read-only and the command access DEFAULT for Vserver vs.

```
cluster1::> security login role delete -role read-only -cmddirname DEFAULT -  
vserver vs
```

## security login role modify

Modify an access control role

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

### Description

The `security login role modify` command modifies an access-control role.

---

## Parameters

**-vserver** <vserver name> - Vserver

This optionally specifies the Vserver name associated with the role.

**-role** <text> - Role Name

This specifies the role that is to be modified.

**-cmddirname** <text> - Command / Directory

This specifies the command or command directory to which the role has access. If you want the default setting, use the special string "DEFAULT" as the value.

**[-access** <Access>] - Access Level

This optionally specifies a new access level for the role. Possible access level settings are none, read-only, and all. The default setting is `all`.

**[-query** <query>] - Query

This optionally specifies the object that the role is allowed to access. The query object must be applicable to the command or directory name specified by `-cmddirname`. The query object must be enclosed in double quotation marks (""), and it must be a valid field name.

## Examples

The following command modifies an access-control role with the role name `read-only` and the command access `DEFAULT` to have the access level `read-only` for Vserver `vs`:

```
cluster1::> security login role modify -role readonly -cmddirname DEFAULT -access  
readonly -vserver vs
```

## security login role show-ontapi

Display the mapping between Data ONTAP APIs and CLI commands

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

## Description

The `security login role show-ontapi` command displays Data ONTAP APIs (ONTAPIs) and the CLI commands that they are mapped to.

---

## Parameters

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

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

| [-instance ] }

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

[**-ontapi** <text>] - ONTAPI Name

Use this parameter to view the corresponding CLI command for the specified API.

[**-command** <text>] - CLI Command

Use this parameter to view the corresponding API or APIs for the specified CLI command.

## Examples

The following command displays all Data ONTAP APIs and their mapped CLI commands:

```
cluster1::> security login role show-ontapi
ONTAPI                                     Command
-----
aggr-add                                  storage aggregate add-disks
aggr-check-spare-low                     storage aggregate check_spare_low
aggr-create                              storage aggregate create
aggr-destroy                             storage aggregate delete
aggr-get-filer-info                      aggr
aggr-get-iter                            storage aggregate show-view
aggr-offline                             storage aggregate offline
aggr-online                              storage aggregate online
aggr-options-list-info                   storage aggregate show
aggr-rename                              storage aggregate rename
aggr-restrict                            storage aggregate restrict
aggr-set-option                          storage aggregate modify
autosupport-budget-get                   system node autosupport budget show
autosupport-budget-get-iter               system node autosupport budget show
autosupport-budget-get-total-records      system node autosupport budget show
autosupport-budget-modify                 system node autosupport budget modify
autosupport-config-get                   system node autosupport show
autosupport-config-get-iter               system node autosupport show
autosupport-config-get-total-records      system node autosupport show
autosupport-config-modify                 system node autosupport modify
Press <space> to page down, <return> for next line, or 'q' to quit...
```

The following example displays all Data ONTAP APIs which are mapped to the specified CLI command:

```
cluster1::> security login role show-ontapi -command version
ONTAPI                                     Command
-----
system-get-ontapi-version                 version
system-get-version                        version
2 entries were displayed.
```

---

The following example displays the CLI command that is mapped to the specified Data ONTAPI API:

```
cluster1::> security login role show-ontapi -ontapi aggr-create
ONTAPI Name: aggr-create
Command: storage aggregate create
```

## security login role show

Show access control roles

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

### Description

The `security login role show` command displays the following information about access-control roles:

- Role name
- Command or command directory to which the role has access
- Access level (none, read-only, or all)
- Query (detailed view only)

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver

Selects the roles that match this parameter value.

[-**role** <text>] - Role Name

Selects the roles that match this parameter value. If this parameter and the `-cmddirname` parameter are both used, the command displays detailed information about the specified access-control role.



---

**[-cmddirname <text>]** - Command / Directory

Selects the roles that match this parameter value. If this parameter and the `-role` parameter are both used, the command displays detailed information about the specified access-control role.

**[-access <Access>]** - Access Level

Selects the roles that match this parameter value.

**[-query <query>]** - Query

Selects the roles that match this parameter value.

## Examples

The example below displays information about all access-control roles:

```
cluster1::> security login role show
```

Vserver	RoleName	Command/Directory	Query	AccessLevel
vs	vsadmin	DEFAULT		none
vs	vsadmin	dashboard health vserver		readonly
vs	vsadmin	job		readonly
vs	vsadmin	job schedule		none
vs	vsadmin	lun		all
vs	vsadmin	network connections		readonly
cluster1	admin	DEFAULT		all
cluster1	readonly	DEFAULT		readonly
cluster1	readonly	volume		none

---

## security login role config modify

Modify local user account restrictions

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

### Description

The `security login role config modify` command modifies user account restrictions.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver name associated with the profile configuration.

**-role** <text> - Role Name

This specifies the role whose account restrictions are to be modified.

**[-username-minlength <integer>]** - Minimum Username Length Required

This specifies the required minimum length of the user name. Possible values range from 3 to 16 characters. The default setting is 3 characters.

**[-username-alfanum {enabled|disabled}]** - Username Alpha-Numeric

This specifies whether a mix of alphabetic and numeric characters are required in the user name. If this parameter is enabled, a user name must contain at least one letter and one number. The default setting is disabled.

**[-passwd-minlength <integer>]** - Minimum Password Length Required

This specifies the required minimum length of a password. Possible values range from 3 to 64 characters. The default setting is 8 characters.

**[-passwd-alfanum {enabled|disabled}]** - Password Alpha-Numeric

This specifies whether a mix of alphabetic and numeric characters is required in the password. If this parameter is enabled, a password must contain at least one letter and one number. The default setting is disabled.

**[-passwd-min-special-chars <integer>]** - Minimum Number of Special Characters Required In The Password

---

This specifies the minimum number of special characters required in a password. Possible values range from 0 to 64 special characters. The default setting is 0, which requires no special characters.

**[-passwd-expiry-time <unsigned32\_or\_unlimited>]** - Password Expires In (Days)

This specifies password expiration in days. A value of 0 means all passwords associated with the accounts in the role expire now. The default setting is unlimited, which means the passwords never expire.

**[-require-initial-passwd-update {enabled|disabled}]** - Require Initial Password Update on First Login

This specifies whether users must change their passwords when logging in for the first time. Initial password changes can be done only through SSH or serial-console connections. The default setting is disabled.

**[-max-failed-login-attempts <integer>]** - Maximum Number of Failed Attempts

This specifies the allowed maximum number of consecutive invalid login attempts. When the failed login attempts reach the specified maximum, the account is automatically locked. The default is 0, which means failed login attempts do not cause an account to be locked.

**[-lockout-duration <integer>]** - Maximum lockout Period (Days)

This optionally specifies the number of days for which an account is locked if the failed login attempts reach the allowed maximum. The default is 0, which means accounts will be locked for 1 day.

**[-disallowed-reuse <integer>]** - Disallow Last 'N' Passwords

This specifies the number of previous passwords that are disallowed for reuse. The default setting is six, meaning that the user cannot reuse any of their last six passwords. The minimum allowed value is 1.

**[-change-delay <integer>]** - Delay Between Password Changes (Days)

This specifies the number of days that must pass between password changes. The default setting is 0.

## Examples

The following command modifies the user-account restrictions for an account with the role name admin for a Vserver named vs. The minimum size of the password is set to 12 characters.

```
cluster1::> security login role config modify -role admin -vserver vs  
-passwd-minlength 12
```

---

## security login role config reset

Reset RBAC characteristics supported on releases later than Data ONTAP 8.1.2

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

### Description

The `security login role config reset` command resets the following role based access control (RBAC) characteristics to their default values. The system prompts you to run this command if you revert to Data ONTAP 8.1.2 or earlier. If you do not reset these characteristics, the revert process will fail.

- Minimum number of special characters required in password ("0")
- Password-expiration time, in days ("unlimited")
- Whether the password must be changed at the initial login ("disabled")
- Maximum number of failed login attempts permitted before the account is locked out ("0")
- Number of days that the user account is locked out after the maximum number of failed login attempts is reached ("0")

### Parameters

None

### Examples

The following command resets the above mentioned RBAC characteristics of all cluster and Vserver roles to their default values.

```
cluster1::> security login role config reset
```

## security login role config show

Show local user account restrictions

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

---

## Description

The `security login role config show` command displays the following information about account restrictions for management-utility user accounts:

- Role name
- Minimum size of the password, in characters
- Whether the password requires alphanumeric characters
- Number of previous passwords that cannot be reused
- Number of days after which a password must be changed

You can display detailed information about the restrictions on a specific account by specifying the `-role` parameter. This adds the following information:

- Minimum length of the user name, in characters
- Whether the user name requires alphanumeric characters
- Minimum length of the password, in characters
- Whether the password requires alphanumeric characters
- Minimum number of special characters required in password
- Password-expiration time, in days
- Whether the password must be changed at the initial login
- Maximum number of failed login attempts permitted before the account is locked out
- Number of minutes that the user account is locked out after the maximum number of failed login attempts is reached
- Number of previous passwords that cannot be reused
- Number of days after which a password must be changed

## Parameters

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

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

| **[-instance ]** }

---

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

**`[-vserver <vserver name>]`** - Vserver

Selects the profile configurations that match this parameter value

**`[-role <text>]`** - Role Name

If this parameter is specified, the command displays detailed information about restrictions for the specified user account.

**`[-username-minlength <integer>]`** - Minimum Username Length Required

Selects the profile configurations that match this parameter value.

**`[-username-alphanum {enabled|disabled}]`** - Username Alpha-Numeric

Selects the profile configurations that match this parameter value. Enabled means a user name must contain both letters and numbers.

**`[-passwd-minlength <integer>]`** - Minimum Password Length Required

Selects the profile configurations that match this parameter value.

**`[-passwd-alphanum {enabled|disabled}]`** - Password Alpha-Numeric

Selects the profile configurations that match this parameter value. Enabled means a password must contain both letters and numbers.

**`[-passwd-min-special-chars <integer>]`** - Minimum Number of Special Characters Required In The Password

Selects the profile configurations that match this parameter value.

**`[-passwd-expiry-time <unsigned32_or_unlimited>]`** - Password Expires In (Days)

Selects the profile configurations that match this parameter value.

**`[-require-initial-passwd-update {enabled|disabled}]`** - Require Initial Password Update on First Login

Selects the profile configurations that match this parameter value.

**`[-max-failed-login-attempts <integer>]`** - Maximum Number of Failed Attempts

Selects the profile configurations that match this parameter value.

**`[-lockout-duration <integer>]`** - Maximum lockout Period (Days)

Selects the profile configurations that match this parameter value.

**`[-disallowed-reuse <integer>]`** - Disallow Last 'N' Passwords

---

Selects the profile configurations that match this parameter value.

**[-change-delay <integer>]** - Delay Between Password Changes (Days)

Selects the profile configurations that match this parameter value.

**Examples**

The example below displays restriction information about all user accounts:

```
cluster1::> security login role config show
----- Password Restrictions -----
Vserver      RoleName      Size AlphaNum NoReuse ChangeDelay
-----
vs            vsadmin       8    enabled      6         0 days
vs            vsadmin-protocol 8    enabled      6         0 days
vs            vsadmin-readonly 8    enabled      6         0 days
vs            vsadmin-volume 8    enabled      6         0 days
cluster1     admin         6    enabled      6         0 days
cluster1     readonly      6    enabled      6         0 days
```

---

## security ssl modify

Modify the SSL configuration for HTTP servers

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

### Description

This command modifies the configuration of encrypted HTTP (SSL) for Vservers in the cluster. Depending on the requirements of the individual node's or cluster's web services (displayed by the `vserver services web show` command), this encryption might or might not be used. If the Vserver does not have a certificate associated with it, SSL will not be available.

### Parameters

**-vserver** <vserver name> - Vserver

Identifies a Vserver for hosting SSL-encrypted web services.

**[-ca <text>]** - Server Certificate Issuing CA

Identifies a Certificate Authority (CA) of a certificate to be associated with the instance of a given Vserver. If this parameter, alongwith serial, is omitted during modification, a self-signed SSL certificate can be optionally generated for that Vserver.

**[-serial <text>]** - Server Certificate Serial Number

Identifies a serial number of a certificate to be associated with the instance of a given Vserver. If this parameter, alongwith ca, is omitted during modification, a self-signed SSL certificate can be optionally generated for that Vserver.

**[-common-name <FQDN or Custom Common Name>]** - Server Certificate Common Name

Identifies the common name (CN) of a certificate to be associated with the instance of a given Vserver. This parameter becomes optional if serial and ca are specified. You can use the `security certificate create` and `security certificate install` commands to add new certificates to Vservers.

Note:

The use of self-signed SSL certificates exposes users to man-in-the-middle security attacks. Where possible, obtain a certificate that is signed by a reputable certificate



---

authority (CA) and use the `security certificate install` command to configure it before enabling SSL on a Vserver.

**`[-server-enabled {true|false}]`** - SSL Server Authentication Enabled

Defines the working condition of SSL server authentication in an instance of the Vserver. Any Vserver with a valid certificate of type server is server-enabled.

**`[-client-enabled {true|false}]`** - SSL Client Authentication Enabled

Defines the working condition of SSL client authentication in an instance of the Vserver. Any Vserver with a valid certificate of type client-ca is client-enabled. It can only be enabled if server-enabled is true.

## Examples

The following example enables SSL server authentication for a Vserver named vs0 with a certificate that has ca as www.example.com and serial as 4F4EB629.

```
cluster1::*>security ssl modify -vserver vs0 -ca www.example.com -serial 4F4EB629  
-server-enabled true
```

The following example disables SSL server authentication for a Vserver name vs0.

```
cluster1::*>security ssl modify -vserver vs0 -server-enabled false
```

The following example enables SSL client authentication for a Vserver named vs0.

```
cluster1::*>security ssl modify -vserver vs0 -client-enabled true
```

The following example disables SSL client authentication for a Vserver named vs0.

```
cluster1::*>security ssl modify -vserver vs0 -client-enabled false
```

## See Also

`security certificate create` `security certificate install` `vserver services web show`

---

## security ssl show

Display the SSL configuration for HTTP servers

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

### Description

This command displays the configuration of encrypted HTTP (SSL) for Vservers in the cluster. Depending on the requirements of the individual node's or cluster's web services (displayed by the `vserver services web show` command), this encryption might or might not be used. If the Vserver does not have a certificate associated with it, SSL will not be available.

### Parameters

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

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

| [-instance ] }

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

[-vserver <vserver name>] - Vserver

Identifies a Vserver for hosting SSL-encrypted web services.

[-ca <text>] - Server Certificate Issuing CA

(Description not available)

[-serial <text>] - Server Certificate Serial Number

(Description not available)

[-common-name <FQDN or Custom Common Name>] - Server Certificate Common Name

(Description not available)

[-server-enabled {true|false}] - SSL Server Authentication Enabled

(Description not available)

---

**[-client-enabled {true|false}] - SSL Client Authentication Enabled**

(Description not available)

**Examples**

The following example displays the configured certificates for Vservers.

```
clus01::security ssl> show
Vserver      Enabled SSL Certificate Name
-----
clus01       false -
n6070-8      true  n6070-8.company.com
n6070-9      true  sample1
3 entries were displayed.
```

**See Also**

vserver services web show

---

## snapmirror abort

Abort an active transfer

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

### Description

The `snapmirror abort` command stops SnapMirror transfers that might have started and have not finished. A SnapMirror transfer is an operation on a given SnapMirror relationship, and the relationship is identified by its destination volume. You identify the SnapMirror relationship with this command and the command aborts the transfer for the relationship, and for load-sharing mirrors, transfers for associated relationships.

Load-sharing mirrors are either up to date and serving data to clients, or they are lagging and not serving data to clients. If the `snapmirror abort` command identifies an up-to-date load-sharing mirror, then SnapMirror transfers to the up-to-date load-sharing mirror and associated up-to-date load-sharing mirrors in the set of load-sharing mirrors are aborted. If the `snapmirror abort` command identifies a lagging load-sharing mirror, then only the SnapMirror transfer associated with the lagging load-sharing mirror is aborted.

After the `snapmirror abort` command successfully completes its operation, the volume on the receiving side of the transfer might contain a restart checkpoint. The restart checkpoint can be used by a subsequent transfer to restart and continue the aborted SnapMirror transfer.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

The use of wildcards in parameter values is not supported from the source Vserver or cluster for relationships with "Relationship Capability" of "8.2 and above".

You can use this command from the source or the destination Vserver or cluster for FlexVol volume relationships or Infinite Volume relationships.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also

---

includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** <[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with

---

"Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-hard | -h [true]]** - Discard Restart Checkpoint

If this option is specified true, the restart checkpoint is discarded and the destination volume is restored to the last Snapshot copy that was successfully transferred. You can use the `-hard` option to discard the restart checkpoint of a previous transfer attempt which forces the subsequent transfer to start with a fresh Snapshot copy on the destination volume. This option can only be used from the destination Vserver or cluster.

**[-foreground | -w [true]]** - Foreground Process

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To stop the active SnapMirror replication to the destination volume `vs2:dept_eng_dp_mirror1`, type the following command:

```
vs2::> snapmirror abort -destination-path  
vs2:dept_eng_dp_mirror1
```

For relationships with "Relationship Capability" of "Pre 8.2", to stop the active SnapMirror replication to the destination volume `clus2://vs2/dept_eng_dp_mirror1`, type the following command:

```
clus2::> snapmirror abort -destination-path  
clus2://vs2/dept_eng_dp_mirror1
```

## See Also

`job stop snapmirror show`

---

## snapmirror break

Make SnapMirror destination writable

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

### Description

The `snapmirror break` command breaks a SnapMirror relationship between a source and destination volume of a data protection mirror. When Data ONTAP breaks the relationship, the destination volume is made a read-write volume and can diverge from the source volume, client redirection is turned off on the destination volume, the restart checkpoint is cleared, and the clients can see the latest Snapshot copy.

Subsequent manual or scheduled SnapMirror updates to the broken relationship will fail until the SnapMirror relationship is reestablished using the `snapmirror resync` command.

This command applies to data protection mirrors. For vault relationships, this command is only intended for use when preparing for a Data ONTAP revert operation (see the `-delete-snapshots` parameter below). This command is not intended for use with load-sharing mirrors.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror break` command must be used from the destination Vserver or cluster.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][[/vserver/]volume>} } - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified.

---

This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-force | -f [true]]** - Force

If this parameter is specified, the command proceeds without prompting for confirmation.

**[-foreground | -w [true]]** - Foreground Process



---

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

**[-delete-snapshots [true]]** - Delete Snapshots for Revert (privilege: advanced)

This parameter is required if this command is used with a vault relationship. Breaking vault relationships is a prerequisite for reverting to a pre-8.2 version of Data ONTAP. This parameter causes break to delete all snapshots on the volume with file system version 8.2 and above.

## Examples

To stop the SnapMirror replication to the destination volume vs2:dept\_eng\_dp\_mirror1, type the following command:

```
vs2::> snapmirror break -destination-path vs2:dept_eng_dp_mirror1
```

For relationships with "Relationship Capability" of "Pre 8.2", to stop the SnapMirror replication to the destination volume clus2://vs2/dept\_eng\_dp\_mirror1, type the following command:

```
clus2::> snapmirror break  
-destination-path clus2://vs2/dept_eng_dp_mirror1
```

## See Also

snapmirror resync   snapmirror show

---

## snapmirror create

Create a new SnapMirror relationship

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

### Description

The `snapmirror create` command creates a SnapMirror relationship between a source and destination volume. You can use this command to create a data protection relationship, a vault relationship, or a load-sharing relationship between FlexVol volumes. You can also use it to create a data protection relationship between Infinite Volumes. Infinite Volumes support only data protection relationships.

Before using this command you typically create a source and destination volume using the `volume create` command. The source volume should be in the online state and a read-write (RW) type. The destination volume should be in the online state and a data protection (DP) type.

You must also take the volume style into consideration when creating SnapMirror relationships. Data ONTAP mirrors FlexVol volumes and Infinite Volumes. It does not mirror FlexCache volumes.

For an Infinite Volume SnapMirror relationship, the destination Infinite Volume size must be greater than or equal to the source Infinite Volume size in bytes. You can verify the size in bytes by running `set -units KB` followed by `volume show`.

If all systems involved are running Data ONTAP version 8.2 and later, a Vserver peering relationship must be set up using the `vserver peer create` command between the source and the destination Vservers in order to create a relationship between the source and destination volumes. To enable interoperability with Data ONTAP version 8.1, if the source volume is on a storage system running Data ONTAP version 8.1 operating in Cluster-Mode, the cluster administrator can create a data protection relationship between the source and destination volumes without a Vserver peering relationship between the source and destination Vservers. These relationships are managed the same way as on Data ONTAP 8.1 and the "Relationship Capability" field, as shown in the output of the `snapmirror show` command, is set to "Pre 8.2".

Note:

SnapMirror relationships, except load-sharing relationships, which are created between two volumes which are both on a storage system running Data ONTAP version 8.2 and later have the "Relationship Capability" field set to "8.2 and above".

---

Load-sharing mirrors must be confined to a single Vserver; they are not allowed to span Vservers. Only the cluster administrator can create a load-sharing relationship. Load-sharing relationships are created with the "Relationship Capability" field set to "Pre 8.2".

A set of load-sharing mirrors can have one or more destination volumes. You create separate SnapMirror relationships between the common source volume and each destination volume to create the set of load-sharing mirrors.

After creating the relationship, the destination volume can be initialized using the `snapmirror initialize` command. The destination volumes in a set of load-sharing mirrors are initialized using the `snapmirror initialize-ls-set` command. Load sharing mirrors are not supported for Infinite Volumes.

The `snapmirror create` command must be used from the destination Vserver or cluster.

## Parameters

**{ -source-path | -S {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

**| -source-cluster <cluster\_name>** - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver <vserver name>** - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume <volume name> }** - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**{ -destination-path {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Destination Path

---

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

[**-type** <snapmirrorType>] - Relationship Type

Specifies the type of SnapMirror relationship that will be created. You can create a data protection relationship (DP), a vault relationship (XDP), or a load-sharing relationship (LS). The default is DP. Infinite Volumes support only data protection relationships (DP).

[**-vserver** <vserver name>] - Managing Vserver

If this optional parameter is specified, designates the managing Vserver. The managing Vserver is authorized to use `snapmirror` commands to manage the SnapMirror relationship. The `-vserver` parameter is currently a reserved parameter.

[**-schedule** <text>] - SnapMirror Schedule

This optional parameter designates the name of the schedule which is used to update the SnapMirror relationship. If you do not designate a schedule, updates are not scheduled, so you must update the SnapMirror relationship manually using the `snapmirror update` command or, in the case of a set of load-sharing mirrors, using the `snapmirror update-ls-set` command.

Note:

---

You define and name a schedule using the `job schedule cron create` command.

The schedules associated with an Infinite Volume SnapMirror relationship should not have an interval shorter than hourly.

**[-policy <sm\_policy>] - SnapMirror Policy**

This optional parameter designates the name of the SnapMirror policy which is associated with the SnapMirror relationship. If you do not designate a policy, the DPDefault policy is applied to data protection relationships and the XDPDefault policy is applied to vault relationships. This parameter is not applicable to relationships with "Relationship Capability" of "Pre 8.2".

Note:

You define and name a policy using the `snapmirror policy create` command.

**[-tries <unsigned32\_or\_unlimited>] - Tries Limit**

This optional parameter determines the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The default is eight times. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2". For relationships with "8.2 and above" capability, the tries limit is controlled by the value of tries in the SnapMirror policy which is associated with the relationship.

Note:

You can set the `-tries` parameter to 0 to disable manual and scheduled updates for the SnapMirror relationship.

**[-throttle | -k <throttleType>] - Throttle (KB/sec)**

This optional parameter limits the network bandwidth used for transfers when the source and destination endpoints belong to different clusters. It configures for the relationship the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters. If no throttle is configured, by default the SnapMirror relationship fully utilizes the network bandwidth available between the clusters. You can also configure the relationship to fully use the network bandwidth available by explicitly setting the throttle to unlimited or 0. The minimum effective throttle value is four Kbytes/sec, so if you specify a throttle value between 1 and 4, it will be treated as 4. The `-throttle` parameter does not affect load-sharing mirrors and other SnapMirror relationships confined to a single cluster.

## Examples

---

To create a data protection mirror between the source endpoint vs1:dept\_eng, and the destination endpoint vs2:dept\_eng\_dp\_mirror2, type the following command:

```
vs2::> snapmirror create -destination-path  
vs2:dept_eng_dp_mirror2 -source-path vs1:dept_eng  
-type DP
```

To create a data protection mirror between the source endpoint clus1://vs1/dept\_eng, and the destination endpoint clus2://vs2/dept\_eng\_dp\_mirror2 when the source cluster is running Data ONTAP 8.1 software, type the following command:

```
clus2::> snapmirror create -destination-path  
clus2://vs2/dept_eng_dp_mirror2 -source-path clus1://vs1/dept_eng  
-type DP
```

To create a load-sharing mirror between the source endpoint clus1://vs1/mkt1, and the destination endpoint clus1://vs1/mkt1\_ls1 with the schedule named 5min used to update the relationship, type the following command:

```
clus1::> snapmirror create -destination-path clus1://vs1/mkt1_ls1  
-source-path clus1://vs1/mkt1 -type LS -schedule 5min
```

## See Also

snapmirror update   snapmirror update-ls-set   job schedule cron create  
snapmirror policy create   volume create   vserver peer create   snapmirror show  
snapmirror initialize   snapmirror initialize-ls-set

---

## snapmirror delete

Delete a SnapMirror relationship

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

### Description

The `snapmirror delete` command removes only the SnapMirror relationship between a source volume and a destination volume, the volumes are not destroyed and Snapshot copies on the volumes are not removed.

The `snapmirror delete` command fails if a SnapMirror transfer for the SnapMirror relationship is in progress for relationships with "Relationship Capability" of "Pre 8.2". For relationships with "8.2 and above" capability the delete will succeed even if a transfer is in progress and the transfer will ultimately stop.

A set of load-sharing mirrors can contain multiple destination volumes, each destination volume having a separate SnapMirror relationship with the common source volume. When used on one of the SnapMirror relationships from the set of load-sharing mirrors, the `snapmirror delete` command deletes the specified SnapMirror relationship from the set of load-sharing mirrors.

The `snapmirror delete` command preserves the read-write or read-only attributes of the volumes of a SnapMirror relationship after the relationship is deleted. Therefore, a read-write volume that was the source of a SnapMirror relationship retains its read-write attributes, and a data protection volume or a load-sharing volume that was a destination of a SnapMirror relationship retains its read-only attributes.

Note:

When a SnapMirror relationship from a set of load-sharing mirrors is deleted, the destination volume becomes a data protection volume and retains the read-only attributes of a data protection volume.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

For relationships with "Relationship Capability" of "8.2 and above", the `snapmirror delete` command must be used from the destination Vserver or cluster. The SnapMirror relationship information is deleted from the destination Vserver, but no cleanup or deletion is performed on the source Vserver. The `snapmirror release`

---

command must be issued on the source Vserver to delete the source relationship information.

For relationships with "Relationship Capability" of "Pre 8.2", you can use this command from the source or from the destination cluster. When used from the destination cluster, the SnapMirror relationship information on the source and destination clusters is deleted. When used from the source cluster, only the SnapMirror relationship information on the source cluster is deleted. The use of `snapmirror delete` on a source cluster is not supported for an Infinite Volume relationships in this release.

## Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.



---

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-force | -f [true]]** - Force

If specified, the delete proceeds even if it cannot clean up all artifacts of the relationship.

**[-foreground | -w [true]]** - Foreground Process

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To delete the SnapMirror relationship with the destination endpoint `vs2:dept_eng_dp_mirror4`, type the following command:

```
vs2::> snapmirror delete -destination-path  
vs2:dept_eng_dp_mirror4
```

For relationships with "Relationship Capability" of "Pre 8.2", to delete the SnapMirror relationship with the destination endpoint `clus2://vs2/dept_eng_dp_mirror4`, type the following command:

```
clus2::> snapmirror delete -destination-path  
clus2://vs2/dept_eng_dp_mirror4
```

## See Also

`snapmirror show` `snapmirror release`

---

## snapmirror initialize-ls-set

Start a baseline load-sharing set transfer

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

### Description

The `snapmirror initialize-ls-set` command initializes and updates a set of load-sharing mirrors. This command is usually used after the `snapmirror create` command is used to create a SnapMirror relationship for each of the destination volumes in the set of load-sharing mirrors. The initial transfers to empty load-sharing mirrors are baseline transfers done in parallel.

Note:

See the `snapmirror update-ls-set` command for a description of baseline and incremental transfers.

The parameter that identifies the set of load-sharing mirrors is the source volume. Data and Snapshot copies are transferred from the source volume to all up-to-date destination volumes in the set of load-sharing mirrors.

Use the `snapmirror initialize` command to add and initialize a new destination volume to an existing set of load-sharing mirrors.

Note:

Even if the load-sharing set only has one mirror, you still need to use the `snapmirror initialize-ls-set` command to initialize the set. The `snapmirror initialize` command can only be used to initialize a new destination volume, if the load-sharing set has already been initialized.

This command is not supported on Infinite Volume snapmirror relationships.

This command is only supported for SnapMirror relationships with the field "Relationship Capability" showing as "Pre 8.2" in the output of the `snapmirror show` command.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

---

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**[-foreground | -w [true]]** - Foreground Process

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To initialize the group of load-sharing mirrors for the source endpoint `//vs1/dept_eng`, type the following command:

```
clus1:> snapmirror initialize-ls-set -source-path //vs1/dept_eng
```

## See Also

`snapmirror create` `snapmirror update-ls-set` `snapmirror initialize` `snapmirror show`

---

## snapmirror initialize

Start a baseline transfer

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

### Description

The `snapmirror initialize` command initializes the destination volume of a SnapMirror relationship. The command behaves differently between data protection, vault, and load-sharing relationships.

For data protection and vault relationships, the `snapmirror initialize` command initializes the destination volume.

For load-sharing relationships, the `snapmirror initialize` command adds and updates a load-sharing mirror to an existing set of load-sharing mirrors. If the command finishes before the start of a scheduled or manual transfer of the set of load-sharing mirrors, the load-sharing mirror is up to date with the set of load-sharing mirrors; otherwise, the load-sharing mirror will be brought up to date at the next scheduled or manual transfer of the set of load-sharing mirrors.

The initial transfer to an empty destination volume is called a baseline transfer. During a baseline transfer for a data protection or vault relationship, the `snapmirror initialize` command takes a Snapshot copy on the source volume to capture the current image of the source volume. For data protection relationships, the `snapmirror initialize` command transfers all of the Snapshot copies up to and including the Snapshot copy created by it from the source volume to the destination volume. For vault relationships, the `snapmirror initialize` command transfers only the Snapshot copy created by it from the source volume to the destination volume.

After the `snapmirror initialize` command successfully completes, the last Snapshot copy transferred is made the exported Snapshot copy on the destination volume.

When an Infinite Volume SnapMirror relationship is initialized, the command will create any needed constituent volumes for the destination Infinite Volume. The Infinite Volume relationship will appear in the `snapmirror show` command output on the source cluster after it is initialized.

You can use the `snapmirror initialize` command to initialize a specific load-sharing mirror that is new to the set of load-sharing mirrors. An initialize of the new load-

---

sharing mirror should bring it up to date with the other up-to-date destination volumes in the set of load-sharing mirrors.

Note:

Using the `snapmirror initialize` command to initialize a set of load-sharing mirrors will not work. Use the `snapmirror initialize-ls-set` command to initialize a set of load-sharing mirrors.

If a SnapMirror relationship does not already exist, that is, the relationship was not created using the `snapmirror create` command, the `snapmirror initialize` command will implicitly create the SnapMirror relationship, with the same behaviors as described for the `snapmirror create` command before initializing the relationship. This implicit create feature is not supported for load-sharing mirrors and not supported for Infinite Volumes.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

For relationships with "Relationship Capability" of "8.2 and above", you can track the progress of the operation using the `snapmirror show` command.

For relationships with "Relationship Capability" of "Pre 8.2", a job will be spawned to operate on the SnapMirror relationship, and the job id will be shown in the command output. The progress of the job can be tracked using the `job show` and `job history show` commands.

The `snapmirror initialize` command must be used from the destination Vserver or cluster.

## Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

---

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

[**-source-snapshot** | **-s** <text>] - Source Snapshot

This optional parameter specifies the Snapshot copy that `snapmirror initialize` will use for the baseline transfer. This parameter is not supported for relationships with "Relationship Capability" of "Pre 8.2". This option is not supported for Infinite Volume SnapMirror relationships.

---

**[-type <snapmirrorType>] - Snapmirror Relationship Type**

Specifies the type of SnapMirror relationship if a relationship is implicitly created. This option is the same as the one used in the `snapmirror create` command.

**[-throttle | -k <throttleType>] - Throttle (KB/sec)**

This optional parameter limits the network bandwidth used for the initialize transfer when the source and destination endpoints belong to different clusters. It sets the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters during the operation. If this parameter is not specified, the throttle value configured for the relationship with the `snapmirror create` or `snapmirror modify` commands will be used. To specify fully using the network bandwidth available between the clusters, set the throttle value to unlimited or 0. The minimum throttle value is four Kbytes/sec, so if you specify a throttle value between 1 and 4, it will be treated as if you specified 4. The `-throttle` option does not affect load-sharing transfers and other transfers confined to a single cluster.

**[-transfer-priority {low|normal}] - Transfer Priority**

This optional parameter specifies the priority at which the transfer runs. The default value for this parameter is the value in the SnapMirror policy associated with this relationship. This parameter is not applicable to relationships with a "Relationship Capability" of "Pre 8.2".

**[-foreground | -w [true]] - Foreground Process**

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To start the initial transfer for the SnapMirror relationship with the destination endpoint `vs2:dept_eng_dp_mirror2` after the relationship has been created with the `snapmirror create` command, type the following command:

```
vs2::> snapmirror initialize -destination-path  
vs2:dept_eng_dp_mirror2
```

For relationships with "Relationship Capability" of "Pre 8.2", to start the initial transfer for the SnapMirror relationship with the destination endpoint `clus2://vs2/dept_eng_dp_mirror2` after the relationship has been created with the `snapmirror create` command, type the following command:

```
clus2::> snapmirror initialize -destination-path  
clus2://vs2/dept_eng_dp_mirror2
```

---

To create a data protection mirror relationship between the source endpoint vs1:dept\_mkt, and the destination endpoint vs2:dep\_mkt\_dp\_mirror, and start the initial transfer, type the following command:

```
vs2::> snapmirror initialize -destination-path  
vs2:dept_mkt_dp_mirror -source-path vs1:dept_mkt
```

To create a data protection mirror relationship between the source endpoint clus1://vs1/dept\_mkt, and the destination endpoint clus2://vs2/dep\_mkt\_dp\_mirror, and start the initial transfer when the source cluster is running Data ONTAP 8.1 software, type the following command:

```
clus2::> snapmirror initialize -destination-path  
clus2://vs2/dep_mkt_dp_mirror -source-path clus1://vs1/dept_mkt
```

## See Also

snapmirror create snapmirror modify snapmirror show snapmirror initialize-ls-set  
job show job history show



---

## snapmirror list-destinations

Display a list of destinations for SnapMirror sources

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

### Description

The `snapmirror list-destinations` command displays information including the destination endpoints, the relationship status, and transfer progress, for SnapMirror relationships whose source endpoints are in the current Vserver if you are in a Vserver context, or the current cluster if you are in a cluster context.

The command might display several relationships that have the same source and destination endpoints, but have different relationship IDs. If this is the case, some of the information is stale. It corresponds to relationships that have been deleted on the destination Vserver or cluster, and have not been released yet on the source Vserver or source cluster.

The relationships and the information displayed are controlled by the parameters that you specify. If no parameters are specified, the command displays the following information associated with each SnapMirror relationship whose source endpoint is in the current Vserver if you are in a Vserver context, or the current cluster if you are in a cluster context:

- Source path
- Relationship Type
- Destination Path
- Relationship Status
- Transfer Progress
- Progress Last Updated
- Relationship ID

Note the following limitations on the information displayed by the `snapmirror list-destinations` command:

- The "Relationship Status" field is not valid after the node hosting the source volume joins the cluster quorum, until at least one transfer is performed on the SnapMirror relationship.

- "Transfer Progress" and "Progress Last Updated" fields are only valid if a Snapshot copy transfer is in progress.

The `-instance` and `-fields` parameters are mutually exclusive and select the fields that are displayed. The `-instance` parameter if specified, displays detailed information about the relationships. The other parameters of the `snapmirror list-destinations` command, select the SnapMirror relationships for which the information is displayed.

## Parameters

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

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

| **[-instance ]** }

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

{ **[-source-path | -S {<[vserver:]volume>|<[cluster:][//vserver/]volume>}]** - Source Path

Selects SnapMirror relationships that have a matching source path name.

| **[-source-vserver <vserver name>]** - Source Vserver

Selects SnapMirror relationships that have a matching source Vserver name.

**[-source-volume <volume name>]** } - Source Volume

Selects SnapMirror relationships that have a matching source volume name.

{ **[-destination-path {<[vserver:]volume>|<[cluster:][//vserver/]volume>}]** - Destination Path

Selects SnapMirror relationships that have a matching destination path name.

| **[-destination-vserver <vserver name>]** - Destination Vserver

Selects SnapMirror relationships that have a matching destination Vserver name.

**[-destination-volume <volume name>]** } - Destination Volume

Selects SnapMirror relationships that have a matching destination volume name.

**[-relationship-id <UUID>]** - Relationship ID

Selects SnapMirror relationships that have a matching relationship identifier.

**[-type <snapmirrorType>]** - Relationship Type

Selects SnapMirror relationships that have a matching relationship type. Possible values are:

- DP
- XDP
- RST

**[-status <mirror status>]** - Relationship Status

Selects SnapMirror relationships that have a matching relationship status. Possible values are:

- Idle
- Transferring

**[-transfer-progress {<integer>[KB|MB|GB|TB|PB]}]** - Transfer Progress

Selects SnapMirror relationships that have a matching transfer progress. This option is not supported for Infinite Volume SnapMirror relationships.

**[-progress-last-updated <MM/DD HH:MM:SS>]** - Timestamp of Last Progress Update

Selects SnapMirror relationships that have a matching transfer progress last updated timestamp. This option is not supported for Infinite Volume SnapMirror relationships.

**[-is-constituent {true|false}]** - Constituent Relationship

Selects SnapMirror relationships that have a matching constituent condition.

**[-source-volume-node <nodename>]** - Source Volume Node Name

Selects SnapMirror relationships that have a matching source volume node name.

## Examples

To display summary information about all relationships whose source endpoints are in the current Vserver, type the following command:

```
vserver1::> snapmirror list-destinations
```

Source Path	Type	Destination Path	Status	Transfer Progress	Progress Last Updated	Relationship ID
vserver1:dp_sl	DP	vserver2:dp_d1	Idle	-	-	06b4327b-954f-11e1-
af65-123478563412						
vserver1:xdp_sl	XDP	vserver2:xdp_d1	Idle	-	-	a9c1db0b-954f-11e1-
af65-123478563412						

2 entries were displayed.

---

To display detailed information about SnapMirror relationships whose source endpoints are in the current Vserver, type the following command:

```
vserver1::> snapmirror list-destinations -instance
      Source Path: vserver1:dp_s1
      Destination Path: vserver2:dp_d1
      Relationship Type: DP
      Relationship Status: Idle
      Transfer Progress: -
      Progress Last Updated: -
      Source Volume Node: node1
      Relationship ID: 06b4327b-954f-11e1-af65-123478563412

      Source Path: vserver1:xdp_s1
      Destination Path: vserver2:xdp_d1
      Relationship Type: XDP
      Relationship Status: Idle
      Transfer Progress: -
      Progress Last Updated: -
      Source Volume Node: node2
      Relationship ID: a9cldb0b-954f-11e1-af65-123478563412

2 entries were displayed.
```

## Restrictions/Limitations

The `snapmirror list-destinations` command does not return information about load-sharing relationships or relationships whose source endpoints were in Data ONTAP 8.1 operating in Cluster-Mode when they were created. You must run the `snapmirror show` command to display information about these relationships.

SnapMirror relationship information on the source Vserver or cluster is populated only after the first successful transfer attempt. Therefore the `snapmirror list-destinations` command, will not return any information about newly created SnapMirror relationships until the baseline transfer completes successfully.

### See Also

`snapmirror show`

---

## snapmirror modify

Modify a SnapMirror relationship

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

### Description

The `snapmirror modify` command allows you to change one or more properties of SnapMirror relationships. The key parameter that identifies any SnapMirror relationship is the destination volume.

For load-sharing mirrors, a change to a property affects all of the SnapMirror relationships in the set of load-sharing mirrors. Destination volumes in a set of load-sharing mirrors do not have individual property settings.

Changes made by the `snapmirror modify` command do not take effect until the next manual or scheduled update of the SnapMirror relationship. Changes do not affect updates that have started and have not finished yet.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror modify` command must be used from the destination Vserver or cluster.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

---

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-vserver** <vserver name>] - Managing Vserver

If this optional parameter is specified, designates the managing Vserver. The managing Vserver is authorized to use some snapmirror commands to manage the SnapMirror relationship. The `-vserver` option is currently a reserved option.

**[-schedule** <text>] - SnapMirror Schedule

---

This optional parameter designates the name of the schedule which is used to update the SnapMirror relationship. If you do not designate a schedule, updates are not scheduled, so you must update the SnapMirror relationship manually using the `snapmirror update` command or, in the case of a set of load-sharing mirrors, using the `snapmirror update-ls-set` command.

Note:

You define and name a schedule using the `job schedule cron create` command.

The schedules associated with an Infinite Volume SnapMirror relationship should not have an interval shorter than hourly.

**[-policy <sm\_policy>]** - SnapMirror Policy

This optional parameter designates the name of the snapmirror policy which is associated with the SnapMirror relationship. If you do not designate a policy, the current policy will be retained. This parameter is not applicable to relationships with "Relationship Capability" of "Pre 8.2".

Note:

You define and name a policy using the `snapmirror policy create` command.

**[-tries <unsigned32\_or\_unlimited>]** - Tries Limit

This optional parameter determines the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The default is eight times. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2". For relationships with "8.2 and above" capability, the tries limit is controlled by the value of tries in the SnapMirror policy which is associated with the relationship.

Note:

You can set the `-tries` parameter to 0 to disable manual and scheduled updates for the SnapMirror relationship.

**[-throttle | -k <throttleType>]** - Throttle (KB/sec)

This optional parameter limits the network bandwidth used for transfers when the source and destination endpoints belong to different clusters. It configures for the relationship the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters. If no throttle is configured, by default the SnapMirror relationship fully utilizes the network bandwidth available between the clusters. You can also configure the relationship to fully use the network bandwidth available by explicitly setting the throttle to unlimited or 0. The minimum effective throttle value is four Kbytes/sec, so if

---

you specify a throttle value between 1 and 4, it will be treated as 4. The `-throttle` parameter does not affect load-sharing mirrors and other SnapMirror relationships confined to a single cluster.

### **[-foreground | -w [true]] - Foreground Process**

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## **Examples**

To change the schedule to halfhour for the SnapMirror relationship with the destination endpoint `vs2:dept_eng_dp_mirror2`, type the following command:

```
vs2::> snapmirror modify -destination-path  
vs2:dept_eng_dp_mirror2 -schedule halfhour
```

For relationships with "Relationship Capability" of "Pre 8.2", to change the schedule to halfhour for the SnapMirror relationship with the destination endpoint `clus2://vs2/dept_eng_dp_mirror2`, type the following command:

```
clus2::> snapmirror modify -destination-path  
clus2://vs2/dept_eng_dp_mirror2 -schedule halfhour
```

## **See Also**

`snapmirror update` `snapmirror update-ls-set` `job schedule cron create`  
`snapmirror policy create` `snapmirror show`



---

## snapmirror promote

Promote the destination to read-write

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

### Description

The `snapmirror promote` command performs a failover to the destination volume of a SnapMirror relationship. This command changes the destination volume from a read-only volume to a read-write volume and makes the destination volume assume the identity of the source volume. The command then destroys the original source volume. The destination volume must be a load-sharing volume. Note that you can promote a load-sharing volume that has been left in read-write state by a previously failed promote operation.

Client accesses are redirected from the original source volume to the promoted destination volume. The view clients see on the promoted destination volume is the latest transferred Snapshot copy, which might lag behind the view clients had of the original source volume before the promote.

The SnapMirror relationship is always deleted as part of the promotion process.

It is possible that the original source volume is the source of multiple SnapMirror relationships. For such a configuration, the promoted destination volume becomes the new source volume of the other SnapMirror relationships.

This command is only supported for SnapMirror relationships with the field "Relationship Capability" showing as "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror promote` command fails if a SnapMirror transfer is in progress for any SnapMirror relationship with "Relationship Capability" of "Pre 8.2" involving the original source volume. It does not fail if a SnapMirror transfer is in progress for a relationship with "Relationship Capability" of "8.2 and above".

This command is not supported on Infinite Volume `snapmirror` relationships.

### Parameters

{ **-source-path** | **-S** {[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also

---

includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with

---

"Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-force | -f [true]]** - Force

If this parameter is specified, the command proceeds without prompting for confirmation.

## Examples

To promote a mirror named `dept_eng_ls_mirror1` to be the source read-write volume for mirroring and client access, type the following command:

```
clus1:> snapmirror promote -destination-path  
//vs1/dept_eng_ls_mirror1 -source-path //vs1/dept_eng -f true
```

## See Also

`snapmirror show`

---

## snapmirror quiesce

Disable future transfers

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

### Description

The `snapmirror quiesce` command disables future transfers for a SnapMirror relationship. If there is no transfer in progress, the relationship becomes "Quiesced".

If there is a transfer in progress, it is not affected, and the relationship becomes "Quiescing" until the transfer completes. If the current transfer aborts, it will be treated like a future transfer and will not restart.

If applied to a load-sharing (LS) SnapMirror relationship, all the relationships in the load-sharing set will be quiesced.

When a SnapMirror relationship is quiesced, it remains quiesced across reboots and fail-overs.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror quiesce` command must be used from the destination Vserver or cluster.

The relationship must exist on the destination Vserver or cluster. When issuing `snapmirror quiesce`, you must specify the destination endpoint. The specification of the source endpoint of the relationship is optional.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

---

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

## Examples

---

To quiesce the SnapMirror relationship with the destination endpoint vs2:dept\_eng\_mirror2, type the following command:

```
vs2::> snapmirror quiesce -destination-path  
vs2:dept_eng_mirror2
```

For relationships with "Relationship Capability" of "Pre 8.2", to quiesce the SnapMirror relationship with the destination endpoint clus2://vs2/dept\_eng\_mirror2, type the following command:

```
clus2::> snapmirror quiesce -destination-path  
clus2://vs2/dept_eng_mirror2
```

## See Also

snapmirror show   snapmirror resume

---

## snapmirror release

Release source information for a SnapMirror relationship

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

### Description

The `snapmirror release` command removes the relationship information from the source Vserver. The command also removes any Snapshot copy owner tags and any Snapshot copies which were created for the specified relationship from the source volume. It does not destroy any volumes. This command must be used from the source Vserver or cluster.

You can use the `snapmirror list-destinations` command to display source Vservers' relationship information.

This command is not supported for SnapMirror relationships with the field "Relationship Capability" showing as "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror release` operation fails if a SnapMirror transfer for the SnapMirror relationship is in a data phase of the transfer.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two formats. The normal format includes the names of the Vserver (vserver), and volume (volume). A format which also includes the name of the cluster (cluster) is also provided for consistency with other `snapmirror` commands. The form of the pathname which includes the cluster name cannot be used when operating in a Vserver context.

| **-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameter `-source-volume` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameter `-source-vserver` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

---

Specifies the destination endpoint of the SnapMirror relationship in one of two formats. The normal format includes the names of the Vserver (vserver), and volume (volume). A format which also includes the name of the cluster (cluster) is also provided for consistency with other snapmirror commands. The form of the pathname which includes the cluster name cannot be used when operating in a Vserver context.

| **-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameter `-destination-volume` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameter `-destination-vserver` must also be specified.

**[-relationship-info-only [true]]** - Remove relationship info only (skip cleanup of snapshots)

If this parameter is specified, the cleanup of Snapshot copies is bypassed and only the source relationship information is removed. It is recommended to specify this parameter only when the source volume is not accessible.

**[-relationship-id <UUID>]** - Relationship ID

This optional parameter specifies the relationship identifier of the relationship. It must be specified when information for more than one relationship with the same source and destination paths is present.

## Examples

To release the source information for the SnapMirror relationship with the destination endpoint `vs2:dept_eng_dp_mirror4`, type the following command:

```
vs1::> snapmirror release -destination-path vs2:dept_eng_dp_mirror4
```

To release the source information for the SnapMirror relationship with the destination endpoint `vs2:dept_eng_dp_mirror4`, and relationship-id `5f91a075-6a72-11e1-b562-123478563412`, type the following command:

```
vs1::> snapmirror release -destination-path vs2:dept_eng_dp_mirror4  
-relationship-id 5f91a075-6a72-11e1-b562-123478563412
```

## See Also

`snapmirror list-destinations` `snapmirror show`



---

## snapmirror restore

Restore a Snapshot copy from a source volume to a destination volume

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

### Description

The `snapmirror restore` command restores the contents of a Snapshot copy from one volume to another volume. This command is not supported for Infinite Volume SnapMirror relationships.

The source of the restore may be a vault destination, a data protection destination (with "Relationship Capability" of "8.2 and above"), or a read-write volume.

A SnapMirror relationship of type RST is created from source volume to another by the `snapmirror restore` command. This relationship lasts for the duration of the restore operation and is deleted when the command completes successfully.

If the destination volume is an empty data protection volume, the `snapmirror restore` command performs a baseline restore. For a baseline restore the following steps are performed:

- Create the RST SnapMirror relationship.
- The contents of the Snapshot copy selected to be restored is copied to the active file system of the destination volume.
- The destination volume is made read-write.
- The RST SnapMirror relationship is deleted.

If the destination volume is a read-write volume, an incremental restore is performed. The incremental restore fails if it cannot find a common Snapshot copy between the source and destination volumes. An incremental restore preserves all Snapshot copies on the destination volume but does not preserve changes to the active file system since the latest Snapshot copy. To preserve changes to the destination volume since the latest Snapshot copy use `volume snapshot create`. Restore is a disruptive operation so client access of the destination volume is not advised for the duration of the operation. For an incremental restore the following steps are performed:

- Create the RST SnapMirror relationship.
- The active file system of the destination volume is reverted to the latest Snapshot copy on the destination volume and the volume is made read-only.

- 
- This Snapshot copy is the exported Snapshot copy and it is the view to which clients are redirected on the destination volume.
  - The contents of the Snapshot copy selected to be restored are copied to the active file system of the destination volume.
  - The destination volume is made read-write.
  - The RST SnapMirror relationship is deleted.

If the volume being restored from is a vault destination, then `snapmirror restore` will copy the latest protected snapshot to the restore target. A specific snapshot may be selected with the `-source-snapshot` parameter. If the target is not empty, this operation will first remove all data and Snapshot copies newer than the latest common Snapshot copy (as a `volume snapshot restore` to that Snapshot copy would do), then perform the restore transfer.

Restoring to an empty read-write volume is not allowed. A volume that is the source or destination endpoint of a SnapMirror load-sharing mirror relationship cannot be the source nor the destination volume for restore. A FlexCache volume may not be the source nor the destination volume for restore.

If `snapmirror restore` fails or is aborted the RST relationship remains. Use `snapmirror show` with the destination volume name to display the reason for the error. An EMS is also generated when a failure occurs. There are two options to recover when restore fails or is aborted:

- Take corrective action suggested by the EMS and reissue the original command.
- Use the original command with `-clean-up-failure` to cancel the request.

When specifying `-clean-up-failure` to cancel an incremental restore request, the following steps are performed:

- If the Snapshot copy has not been restored to the destination volume, all data copied to the active file system by `snapmirror restore` to the destination volume is reverted.
- The destination volume is made read-write.
- The RST SnapMirror relationship is deleted.

When specifying `-clean-up-failure` to cancel a baseline restore request, the following steps are performed:

- If the Snapshot copy has been restored to the destination volume, the volume is made read-write.

- 
- The RST SnapMirror relationship is deleted.

The `snapmirror restore` command must be used from the destination Vserver or cluster.

## Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint in one of two formats. The basic format includes the names of the Vserver (vserver) and volume (volume). A format which also includes the name of the cluster (cluster) is supported for consistency with other `snapmirror` commands. The form of the pathname which includes the cluster name is not valid when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the cluster in which the source volume resides. This parameter is not needed; it is provided for consistency with other `snapmirror` commands. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is not valid when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, the `-source-volume` parameter must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` parameter must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint in one of two formats. The basic format includes the names of the Vserver (vserver) and volume (volume). A format that also includes the name of the cluster (cluster) is supported for consistency with other `snapmirror` commands. The form of the pathname which includes the cluster name is not valid when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the cluster in which the destination volume resides. This parameter is not needed; it is provided for consistency with other `snapmirror` commands. If this parameter is specified, the `-destination-vserver` and `-destination-volume` parameters must also be specified. This parameter is not valid when operating in a

---

Vserver context. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2".

**-destination-vsriver <vserver name>** - Destination Vserver

Specifies the destination Vserver. If this parameter is specified, the `-destination-volume` parameter must also be specified.

**-destination-volume <volume name> }** - Destination Volume

Specifies the destination volume. If this parameter is specified, the `-destination-vsriver` parameter must also be specified.

**[-source-snapshot | -s <text>]** - Source Snapshot

This optional parameter identifies the Snapshot copy to be restored from the source volume to the destination volume. The default value is the latest snapshot on the source volume.

**[-throttle | -k <throttleType>]** - Throttle (KB/sec)

This optional parameter limits the network bandwidth used for the restore transfer when the source and destination volumes belong to different clusters. It sets the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters during the operation. To specify fully using the network bandwidth available between the clusters, set the throttle value to unlimited or 0. The minimum throttle value is four Kbytes/sec, so if you specify a throttle value between 1 and 4, it will be treated as if you specified 4.

**[-transfer-priority {low|normal}]** - Transfer Priority

This optional parameter specifies the priority at which the transfer runs. The default value for this parameter is `normal`.

**[-disable-storage-efficiency [true]]** - Disable storage efficient transfer

The default behavior of restore is to preserve storage efficiency when possible. Use this optional parameter to turn off storage efficiency for data transferred over the wire and written to the destination volume.

**[-clean-up-failure [true]]** - Clean Up after Failure

Use this optional parameter to recover from an aborted or failed restore operation. If the destination volume was read-write prior to the failed or aborted restore operation, it is converted back to read-write if necessary while removing all data transferred or copied during the restore operation. Any residual temporary RST relationship is also removed from the destination Vserver. An attempt is made to remove any residual temporary RST relationship from the source Vserver.

**[-tries <unsigned32\_or\_unlimited>]** - Tries Limit

---

Specifies the total number of attempts to transfer data in cases where a transfer is interrupted by an error that SnapMirror can recover from. The value of this parameter must be a positive integer or unlimited.

**[-force | -f [true]]** - Force

If this parameter is specified, the command proceeds without prompting for confirmation.

## Examples

The following example does an incremental restore between the restore source volume vs2:dept\_eng\_dp\_mirror2 and the restore destination volume vs1:dept\_eng:

```
vs1::> snapmirror restore -destination-path vs1:dept_eng
      -source-path vs2:dept_eng_dp_mirror2 -source-snapshot snap3
Warning: All data newer than Snapshot copy snap6 on volume vs1:dept_eng
        will be deleted.
Do you want to continue? {y|n}: y
[Job 34] Job is queued: snapmirror restore from source vs2:dept_eng_dp_mirror2
        for the snapshot snap3.
```

## See Also

snapmirror volume snapshot create volume snapshot restore snapmirror show

---

## snapmirror resume

Enable future transfers

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

### Description

The `snapmirror resume` command enables future transfers for a SnapMirror relationship that has been quiesced.

If there is a scheduled transfer for the relationship, it will be triggered on the next schedule. If there is a restart checkpoint, it will be re-used if possible.

If applied on a load-sharing (LS) SnapMirror relationship, it enables future transfers for all the relationships in the load-sharing set.

When a quiesced SnapMirror relationship is resumed, future transfers remain enabled across reboots and fail-overs.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

The `snapmirror resume` command must be used from the destination Vserver or cluster.

The relationship must exist on the destination Vserver or cluster. When issuing `snapmirror resume`, you must specify the destination endpoint. The specification of the source endpoint of the relationship is optional.

### Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified.

---

This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

{ **-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-destination-cluster** <cluster\_name> - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

## Examples

---

To re-enable future transfers for the SnapMirror relationship with the destination endpoint vs2:dept\_eng\_dp\_mirror2 that has been previously quiesced, type the following command:

```
vs2::> snapmirror resume -destination-path  
vs2:dept_eng_dp_mirror2
```

To re-enable future transfers for the SnapMirror relationship with the destination endpoint clus2://vs2/dept\_eng\_dp\_mirror2 that has been previously quiesced, type the following command:

```
clus2::> snapmirror resume -destination-path  
clus2://vs2/dept_eng_dp_mirror2
```

## See Also

snapmirror show   snapmirror quiesce



---

## snapmirror resync

Start a resynchronize operation

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

### Description

The `snapmirror resync` command establishes or reestablishes a mirroring relationship between a source volume and a destination volume, typically in the following cases:

- The destination mirror is broken (that is, the destination volume is a read-write volume and no longer a data protection mirror). After the `snapmirror resync` command completes, the destination volume is made a data protection mirror and the mirror can be manually updated or scheduled for updates.
- `snapmirror update` command failed because the required common Snapshot copy was deleted on the source volume.
- The volumes are the first and third endpoints in a cascade chain of relationships and they have a common Snapshot copy. In this case, `snapmirror resync` may implicitly create the SnapMirror relationship between them.

Attention:

The `snapmirror resync` command can cause data loss on the destination volume because the command can remove the exported Snapshot copy on the destination volume.

The default behavior of the `snapmirror resync` command is defined as follows:

- Finds the most recent common Snapshot copy between the source and destination volumes, removes Snapshot copies on the destination volume that are newer than the common Snapshot copy and mounts the destination volume as a DP volume with the common Snapshot copy as the exported Snapshot copy.
- For data protection relationships, takes a Snapshot copy of the source volume to capture the current image and transfers Snapshot copies that are newer than the common Snapshot copy from the source volume to the destination volume. For vault relationships, transfers Snapshot copies newer than the common Snapshot

---

copy according to the relationship policy, i.e., Snapshot copies will match rules associated with the policy as defined by the `snapmirror policy` commands.

The `snapmirror resync` command supports an optional parameter "preserve". The parameter "preserve" is only supported for vault relationships. When used, the parameter "preserve" changes the behavior of `snapmirror resync` command. Changed behavior of the command can be described as follows:

- Finds the most recent common Snapshot copy between the source and destination volumes, preserves all Snapshot copies on the destination volume that are newer than the common Snapshot copy, and mounts the destination volume as a DP volume with the common Snapshot copy as the exported Snapshot copy.
- Performs a local rollback transfer to make a copy of the common Snapshot copy on the destination volume and establish it as the latest Snapshot copy on the destination volume. The command then transfers all Snapshot copies that are newer than the common Snapshot copy, from the source volume to the destination volume. The command only transfers Snapshot copies that match the vault relationship's policy, i.e., Snapshot copies will match rules associated with the policy as defined by the `snapmirror policy` commands.

If a SnapMirror relationship does not already exist, that is, the relationship was not created using the `snapmirror create` command, the `snapmirror resync` command will implicitly create the SnapMirror relationship, with the same behaviors as described for the `snapmirror create` command before resynchronizing the relationship. This might happen in a cascade chain of relationships where two volumes share a Snapshot copy because one volume is the destination of the other volume.

For Infinite Volumes, you must create Infinite Volume SnapMirror relationships using the `snapmirror create` command before you run the `snapmirror resync` command. The `snapmirror resync` command does not implicitly create the SnapMirror relationship.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

For relationships with "Relationship Capability" of "8.2 and above", you can track the progress of the operation using the `snapmirror show` command.

For relationships with "Relationship Capability" of "Pre 8.2", a job will be spawned to operate on the SnapMirror relationship, and the job id will be shown in the command output. The progress of the job can be tracked using the `job show` and `job history show` commands.

The `snapmirror resync` command fails if the destination volume does not have a Snapshot copy in common with the source volume.

---

The `snapmirror resync` command does not work on load-sharing mirrors.

The `snapmirror resync` command must be used from the destination Vserver or cluster.

## Parameters

**{ -source-path | -S {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

**| -source-cluster <cluster\_name>** - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver <vserver name>** - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume <volume name> }** - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**{ -destination-path {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

**| -destination-cluster <cluster\_name>** - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship

---

Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-source-snapshot | -s <text>]** - Source Snapshot

This optional parameter specifies a Snapshot copy to transfer. The default behavior, in many cases, is that Data ONTAP creates a new Snapshot copy and uses it as the basis for determining what data are replicated; with this option, the specified Snapshot copy will be used instead. For vault relationships, the specified Snapshot copy may be newer or older than the common Snapshot copy; for data protection relationships, the specified Snapshot copy must be newer than the latest common Snapshot copy. This parameter is not supported for relationships with "Relationship Capability" of "Pre 8.2".

**[-type <snapmirrorType>]** - Snapmirror Relationship Type

Specifies the type of SnapMirror relationship if a relationship is implicitly created. The default is data protection (DP).

**[-force | -f [true]]** - Force

If this parameter is specified, the command proceeds without prompting for confirmation.

**[-throttle | -k <throttleType>]** - Throttle (KB/sec)

This optional parameter limits the network bandwidth used for the resync transfer when the source and destination endpoints belong to different clusters. It sets the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters during the operation. If this parameter is not specified, the throttle value configured for the relationship with the `snapmirror create` or `snapmirror modify` commands will be used. To specify fully using the network bandwidth available between the clusters, set the throttle value to unlimited or 0. The minimum throttle value is four Kbytes/sec, so if you specify a throttle value between 1 and 4, it will be treated as if you specified 4. The `-throttle` option does not affect load-sharing transfers and other transfers confined to a single cluster.

**[-transfer-priority {low|normal}]** - Transfer Priority

---

This optional parameter specifies the priority at which the transfer runs. The default value for this parameter is the value in the SnapMirror policy associated with this relationship. This parameter is not applicable to relationships with a "Relationship Capability" of "Pre 8.2".

**[-preserve [true]] - Preserve**

This parameter is only supported for vault relationships. It is not supported for data protection and load-sharing relationships. When specified, it changes the behavior of `snapmirror resync` to preserve Snapshot copies on the destination volume that are newer than the latest common Snapshot copy. This parameter is not supported for relationships with "Relationship Capability" of "Pre 8.2". This option is not supported for Infinite Volume SnapMirror relationships.

**[-foreground | -w [true]] - Foreground Process**

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To reestablish mirroring for the destination endpoint `vs2:dept_mkt_mirror` that has been previously broken off with the `snapmirror break` command, type the following command:

```
vs2::> snapmirror resync -destination-path  
vs2:dept_mkt_dp_mirror
```

For relationships with "Relationship Capability" of "Pre 8.2", to reestablish mirroring for the destination endpoint `clus2://vs2/dept_mkt_mirror` that has been previously broken off with the `snapmirror break` command, type the following command:

```
clus2::> snapmirror resync -destination-path  
clus2://vs2/dept_mkt_dp_mirror
```

To create a SnapMirror relationship and reestablish mirroring between the destination endpoint named `vs2:dept_eng_dp_mirror2` and the source endpoint named `vs1:dept_eng`, type the following command:

```
vs2::> snapmirror resync -destination-path  
vs2:dept_eng_dp_mirror2 -source-path vs1:dept_eng
```

To create a SnapMirror relationship and reestablish mirroring between the destination endpoint named `clus2://vs2/dept_eng_dp_mirror2` and the source endpoint named `clus1://vs1/dept_eng` when the source cluster is running Data ONTAP 8.1 software, type the following command:

```
clus2::> snapmirror resync -destination-path
```

---

```
clus2://vs2/dept_eng_dp_mirror2 -source-path clus1://vs1/dept_eng
```

## See Also

snapmirror create   snapmirror modify   snapmirror update   snapmirror policy  
snapmirror show   job show   job history show   snapmirror break

---

## snapmirror show

Display a list of SnapMirror relationships

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

### Description

The `snapmirror show` command displays information associated with SnapMirror relationships. By default, the command displays the following information:

- Source path
- Relationship Type
- Destination Path
- Mirror State
- Relationship Status
- Total Progress
- Healthy
- Progress Last Updated

For backward compatibility with Data ONTAP 8.1 operating in Cluster-Mode, SnapMirror relationships, which match one of the following conditions are managed as on Data ONTAP 8.1 operating in Cluster-Mode: (1) The relationship is of type load-sharing; (2) The source endpoint of the relationship is on a remote Data ONTAP 8.1 cluster; (3) The local cluster was upgraded from Data ONTAP 8.1 operating in Cluster-Mode, and the relationship was created before the upgrade. These relationships have the same limitations as on Data ONTAP 8.1 operating in Cluster-Mode. Especially, they support the same set of information fields. The "Relationship Capability" field is set to "Pre 8.2" for these relationships.

The `snapmirror show` command displays information for SnapMirror relationships whose destination endpoints are in the current Vserver if you are in a Vserver context, or in the current cluster if you are in a cluster context. For backward compatibility with Data ONTAP 8.1 operating in Cluster-Mode, the command also displays information for SnapMirror relationships with the "Relationship Capability" of "Pre 8.2", and whose source endpoints are in the current Vserver or cluster, and destination endpoints are in different Vservers or clusters. You must use the `snapmirror list-destinations`

---

command to display information for SnapMirror relationships whose source endpoints are in the current Vserver or current cluster.

Some of the SnapMirror relationship information is cached. The `snapmirror show` command returns the cached information.

The `-instance` and `-fields` parameters are mutually exclusive and select the information fields that are displayed. The other parameters to the `snapmirror show` command select the SnapMirror relationships for which information is displayed. The `-instance` displays detailed information fields including:

```
Source Path: Path of the source endpoint.
Destination Path: Path of the destination endpoint.
Relationship Type: Type of the SnapMirror relationship. May be
                  one of the following:
                  - DP: Data protection relationship.
                  - LS: Load-sharing relationship.
                  - XDP: Vault relationship.
                  - RST: Temporary relationship created
                        during a restore operation, and
                        deleted if the operation completes
                        successfully.
                  - TDP: 7-mode to Cluster-Mode transition
                        data protection relationship.
Relationship Status: Status of the SnapMirror relationship.
                  May be one of the following:
                  - Idle: No transfer operation is in
                        progress and future transfers are
                        not disabled.
                  - Queued: A transfer operation has been
                        accepted and queued in the system,
                        and future transfers are not
                        disabled.
                  - Transferring: A transfer operation is in
                        progress and future transfers are not
                        disabled.
                  - Preparing: Pre-transfer phase for
                        Vault incremental transfers.
                        For Vault relationships only.
                  - Finalizing: Post-transfer phase for
                        Vault incremental transfers.
                        Network traffic will be low as
                        processing is primarily on the
                        destination volume.
                        For Vault relationships only.
                  - Aborting: A transfer abort operation
                        that may include the removal of the
                        checkpoint is underway. Future
                        transfers are not disabled. Only
                        for relationships with
                        "Relationship Capability"
                        of "8.2 and above".
                  - Quiesced: No transfer operation is in
                        progress and future transfers are
                        disabled.
                  - Quiescing: A transfer operation is in
                        progress and future transfers
                        are disabled.
                  - Checking: Destination volume is
                        undergoing a diagnostic check,
                        no transfer is in progress, and
                        future transfers are not disabled.
                        Only for relationships with
                        "Relationship Capability"
                        of "Pre 8.2".
Mirror State: State of the destination volume. May be one
              of the following:
              - Uninitialized: Destination volume has not
                    been initialized.
              - Snapmirrored: Destination volume has been
                    initialized and is ready to
                    receive SnapMirror updates.
              - Broken-off: Destination volume is RW
```



---

and snapshots are present.

Healthy: Condition of the relationship. May be one of the following:

- true: The SnapMirror relationship is healthy. It has not missed a scheduled transfer, or experienced a manual update failure.
- false: The SnapMirror relationship is not healthy. It has missed a scheduled transfer, or has experienced a manual update failure.

Unhealthy Reason: Reason the SnapMirror relationship is not healthy. Only for relationships with "Relationship Capability" of "8.2 and above"

Newest Snapshot: Name of the newest Snapshot copy on the destination volume.

Newest Snapshot Timestamp: Timestamp of the newest Snapshot copy.

Exported Snapshot: Name of the exported Snapshot copy on the destination volume.

Exported Snapshot Timestamp: Timestamp of the exported Snapshot copy.

Lag Time: Time since the exported Snapshot copy was created. It is displayed in the format: hours:minutes:seconds. Only for relationships with "Relationship Capability" of "8.2 and above".

Transfer Type: Type of the current transfer operation. May be one of the following:

- initialize
- update
- resync
- restore

Only for relationships with "Relationship Capability" of "8.2 and above".

Transfer Snapshot: Name of the Snapshot copy being transferred.

Snapshot Progress: Amount of data transferred for the transfer snapshot.

Total Progress: Total amount of data transferred for the current transfer operation.

Transfer Error: Possible transient error condition if any, encountered by the current transfer operation. Only for relationships with "Relationship Capability" of "8.2 and above".

Current Throttle: The maximum transfer rate in Kilobytes per second, used for the current transfer between clusters. Only for relationships with "Relationship Capability" of "8.2 and above".

Current Transfer Priority: Priority assigned to the current transfer. Possible values are:

- low
- normal

Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer Type: Type of the previous transfer operation:

- initialize
- update
- resync
- restore

Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer Size: Total amount of data transferred during the the previous transfer operation if it was successful. Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer Duration: Duration of the previous transfer operation if it was successful. Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer From: Source endpoint of the previous transfer operation.

---

---

Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer End Timestamp: Timestamp of the end of the previous transfer operation.

Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer Error: Cause of the failure of the previous transfer operation.

Only for relationships with "Relationship Capability" of "8.2 and above".

Last Transfer Error Codes: Set of ONTAP internal error codes providing information on the context of the previous transfer failure. This field is used for diagnostic purposes only.

Only for relationships with "Relationship Capability" of "8.2 and above".

Relationship Capability: Management and control compatibility:

- "Pre 8.2": Management and control of the relationship is compatible with Data ONTAP 8.1 operating in Cluster-Mode.
- "8.2 and above": Full support of Data ONTAP 8.2 or later operating in Cluster-Mode SnapMirror relationship management and control.

Relationship ID: The unique identifier of the relationship.

Only for relationships with "Relationship Capability" of "8.2 and above".

Throttle (KB/sec): Configured maximum transfer rate for cross-cluster transfers.

SnapMirror Policy: Name of the SnapMirror policy associated with the relationship.

Only for relationships with "Relationship Capability" of "8.2 and above".

SnapMirror Schedule: Name of the schedule (empty if there is no schedule) associated with the relationship.

Tries Limit: Maximum number of times a transfer will be tried.

Only for relationships with "Relationship Capability" of "pre 8.2".

Constituent Relationship: Whether or not the SnapMirror relationship is between Infinite Volume constituent volumes. May be:

- true: The relationship is between constituent volumes.
- false: The relationship is not between constituent volumes.

Destination Volume Node: Node which owns the destination volume of the relationship.

Only for relationships with "Relationship Capability" of "8.2 and above".

## Parameters

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

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

| [-instance ] }

---

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

{ **[-source-path | -S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>}} - Source Path

Select SnapMirror relationships that have a matching source path name.

| **[-source-cluster** <cluster\_name>] - Source Cluster

Select SnapMirror relationships that have a matching source cluster name.

**[-source-vserver** <vserver name>] - Source Vserver

Select SnapMirror relationships that have a matching source Vserver name.

**[-source-volume** <volume name>] } - Source Volume

Select SnapMirror relationships that have a matching source volume name.

{ **[-destination-path** {<[vserver:]volume>|<[cluster:][//vserver/]volume>}} - Destination Path

Select SnapMirror relationships that have a matching destination path name.

| **[-destination-cluster** <cluster\_name>] - Destination Cluster

Select SnapMirror relationships that have a matching destination cluster name.

**[-destination-vserver** <vserver name>] - Destination Vserver

Select SnapMirror relationships that have a matching destination Vserver name.

**[-destination-volume** <volume name>] } - Destination Volume

Select SnapMirror relationships that have a matching destination volume name.

**[-type** <snapmirrorType>] - Relationship Type

Select SnapMirror relationships that have a matching relationship type. Infinite Volume supports only DP snapmirror relationships. Possible values are:

- DP
- LS
- XDP
- TDP
- RST

**[-vserver** <vserver name>] - Managing Vserver

---

Select SnapMirror relationships that have a matching managing Vserver name. The `-vserver` option is currently a reserved option.

**[-schedule <text>]** - SnapMirror Schedule

Select SnapMirror relationships that have a matching schedule.

**[-policy <sm\_policy>]** - SnapMirror Policy

Select SnapMirror relationships that have a matching SnapMirror policy.

**[-tries <unsigned32\_or\_unlimited>]** - Tries Limit

Select SnapMirror relationships that have a matching tries limit.

**[-throttle | -k <throttleType>]** - Throttle (KB/sec)

Select SnapMirror relationships that have a matching throttle.

**[-current-throttle <throttleType>]** - Current Transfer Throttle (KB/sec)

Select SnapMirror relationships that have a matching current throttle.

**[-state <mirror state>]** - Mirror State

Select SnapMirror relationships that have a matching mirror state. Possible values are:

- Uninitialized
- Snapmirrored
- Broken-off

**[-status <mirror status>]** - Relationship Status

Select SnapMirror relationships that have a matching relationship status. Possible values are:

- Idle
- Queued
- Transferring
- Preparing
- Finalizing
- Aborting
- Quiesced
- Quiescing

- 
- Checking

Status values Finalizing, Checking and Waiting are not supported for Infinite Volume SnapMirror relationships.

**[-transfer-snapshot <text>]** - Transfer Snapshot

Select SnapMirror relationships that have a matching transfer Snapshot copy.

**[-snapshot-progress {<integer>[KB|MB|GB|TB|PB]}]** - Snapshot Progress

Select SnapMirror relationships that have a matching Snapshot progress.

**[-total-progress {<integer>[KB|MB|GB|TB|PB]}]** - Total Progress

Select SnapMirror relationships that have a matching total progress.

**[-snapshot-checkpoint {<integer>[KB|MB|GB|TB|PB]}]** - Snapshot Checkpoint

Select SnapMirror relationships that have a matching Snapshot copy checkpoint.

**[-newest-snapshot <text>]** - Newest Snapshot

Select SnapMirror relationships that have a matching newest Snapshot copy.

**[-newest-snapshot-timestamp <MM/DD HH:MM:SS>]** - Newest Snapshot Timestamp

Select SnapMirror relationships that have a matching newest Snapshot copy timestamp.

**[-exported-snapshot <text>]** - Exported Snapshot

Select SnapMirror relationships that have a matching exported Snapshot copy name. For load-sharing mirror relationships, if the exported-snapshot field for a relationship has a dash (-), the load-sharing mirror is lagging behind the up-to-date mirrors in the set.

**[-exported-snapshot-timestamp <MM/DD HH:MM:SS>]** - Exported Snapshot Timestamp

Select SnapMirror relationships that have a matching exported Snapshot copy timestamp.

**[-healthy {true|false}]** - Healthy

Select SnapMirror relationships that have a matching healthy condition.

**[-relationship-id <UUID>]** - Relationship ID

Select SnapMirror relationships that have a matching relationship ID.

**[-current-transfer-type {initialize|update|resync|restore|check}]** - Transfer Type

Select SnapMirror relationships that have a matching current transfer type. Transfer type Check is not supported for Infinite Volume SnapMirror relationships.

---

**[-current-transfer-error <text>]** - Transfer Error

Select SnapMirror relationships that have a matching current transfer error.

**[-last-transfer-type {initialize|update|resync|restore|check}]** - Last Transfer Type

Select SnapMirror relationships that have a matching last transfer type.

**[-last-transfer-error <text>]** - Last Transfer Error

Select SnapMirror relationships that have a matching last transfer error.

**[-last-transfer-size {<integer>[KB|MB|GB|TB|PB]}]** - Last Transfer Size

Select SnapMirror relationships that have a matching last transfer size.

**[-last-transfer-duration <[[<hours>:]<minutes>:]<seconds>>]** - Last Transfer Duration

Select SnapMirror relationships that have a matching last transfer duration.

**[-last-transfer-from <text>]** - Last Transfer From

Select SnapMirror relationships that have a matching last transfer source.

**[-last-transfer-end-timestamp <MM/DD HH:MM:SS>]** - Last Transfer End Timestamp

Select SnapMirror relationships that have a matching last transfer end timestamp.

**[-unhealthy-reason <text>]** - Unhealthy Reason

Select SnapMirror relationships that have a matching unhealthy reason. This option is not supported for Infinite Volume SnapMirror relationships.

**[-progress-last-updated <MM/DD HH:MM:SS>]** - Progress Last Updated

Select SnapMirror relationships that have a matching progress last updated.

**[-relationship-capability <text>]** - Relationship Capability

Select SnapMirror relationships that have a matching relationship capability.

**[-lag-time <[[<hours>:]<minutes>:]<seconds>>]** - Lag Time

Select SnapMirror relationships that have a matching lag time.

**[-current-transfer-priority {low|normal}]** - Current Transfer Priority

Select SnapMirror relationships that have a matching current transfer priority.

**[-is-smtape-op {true|false}]** - SMTape Operation

Select SnapMirror relationships that have a matching smtape operation. This option is not supported for Infinite Volume SnapMirror relationships.

**[-is-constituent {true|false}]** - Constituent Relationship

---

Select SnapMirror relationships that have a matching constituent condition.

**[-destination-volume-node <nodename>]** - Destination Volume Node Name

Select SnapMirror relationships that have a matching destination volume node name.

## Examples

The example below displays summary information for all SnapMirror relationships with destination endpoints in the current cluster:

```
cluster2::> snapmirror show
Source      Destination  Mirror  Relationship  Total  Healthy  Last
Path        Type        Path    State         Status Progress Updated
-----
cluster2-vs1:dp_src1
DP          cluster2-vs2:dp_dst1
Snapmirrored
Idle
-          true    -
cluster2-vs1:xdp_src1
XDP        cluster2-vs2:xdp_dst1
Snapmirrored
Idle
-          true    -
cluster2://cluster2-vs1/ls_src1
LS         cluster2://cluster2-vs1/ls_mr1
Snapmirrored
Idle
-          true    -
cluster2://cluster2-vs1/ls_mr2
Snapmirrored
Idle
-          true    -
4 entries were displayed.
```

The example below displays detailed information for the SnapMirror relationship with the destination endpoint cluster2-vs2:dp\_dst1.

```
cluster2::> snapmirror show -destination-path cluster2-vs2:dp_dst1
Source Path: cluster2-vs1:dp_src1
Destination Path: cluster2-vs2:dp_dst1
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot:
snapmirror.3d19af37-8f5e-11e1-8c83-123478563412_2147484676.2012-04-27_025137
Newest Snapshot Timestamp: 04/27 02:51:42
Exported Snapshot:
snapmirror.3d19af37-8f5e-11e1-8c83-123478563412_2147484676.2012-04-27_025137
Exported Snapshot Timestamp: 04/27 02:51:42
Healthy: true
Unhealthy Reason: -
Constituent Relationship: false
Destination Volume Node: cluster2-node1
Relationship ID: cdc70a81-8f5f-11e1-8392-123478563412
Transfer Type: -
Transfer Error: -
Current Throttle: -
Current Transfer Priority: -
Last Transfer Type: update
Last Transfer Error: -
Last Transfer Size: 530.2MB
Last Transfer Duration: 0:2:53
Last Transfer From: cluster2-vs1:dp_src1
Last Transfer End Timestamp: 04/27 02:51:45
```

---

```
Progress Last Updated: -
Relationship Capability: 8.2 and above
Lag Time: 133:50:40
SnapMirror Policy: DPDefault
```

The example below displays detailed information for SnapMirror relationships with the Relationship Capability of "Pre 8.2" source or destination endpoints in the current cluster.

```
cluster2::> snapmirror show -relationship-capability "Pre 8.2" -instance

    Source Path: cluster2://cluster2-vs1/ls_src1
    Destination Path: cluster2://cluster2-vs1/ls_mr1
    Relationship Type: LS
    SnapMirror Schedule: -
      Tries Limit: 8
    Throttle (KB/sec): unlimited
    Mirror State: Snapmirrored
    Relationship Status: Idle
    Transfer Snapshot: -
    Snapshot Progress: -
    Total Progress: -
    Snapshot Checkpoint: -
    Newest Snapshot:
snapmirror.3d4e52c5-8f5c-11e1-8392-123478563412_3_2147484684.2012-05-02_163506
    Newest Snapshot Timestamp: 05/02 16:35:06
    Exported Snapshot:
snapmirror.3d4e52c5-8f5c-11e1-8392-123478563412_3_2147484684.2012-05-02_163506
    Exported Snapshot Timestamp: 05/02 16:35:06
      Healthy: true
    Unhealthy Reason: -
    Constituent Relationship: false
    Destination Volume Node: cluster2-node1
    Relationship ID: -
    Transfer Type: -
    Transfer Error: -
    Last Transfer Type: update
    Last Transfer Error: -
    Last Transfer Size: -
    Last Transfer Duration: -
    Last Transfer From: -
Last Transfer End Timestamp: -
    Progress Last Updated: -
    Relationship Capability: Pre 8.2
      Lag Time: -
    SnapMirror Policy: -

    Source Path: cluster2://cluster2-vs1/ls_src1
    Destination Path: cluster2://cluster2-vs1/ls_mr2
    Relationship Type: LS
    SnapMirror Schedule: -
      Tries Limit: 8
    Throttle (KB/sec): unlimited
    Mirror State: Snapmirrored
    Relationship Status: Idle
    Transfer Snapshot: -
    Snapshot Progress: -
    Total Progress: -
    Snapshot Checkpoint: -
    Newest Snapshot:
snapmirror.3d4e52c5-8f5c-11e1-8392-123478563412_3_2147484684.2012-05-02_163506
    Newest Snapshot Timestamp: 05/02 16:35:06
    Exported Snapshot:
snapmirror.3d4e52c5-8f5c-11e1-8392-123478563412_3_2147484684.2012-05-02_163506
    Exported Snapshot Timestamp: 05/02 16:35:06
      Healthy: true
    Unhealthy Reason: -
    Constituent Relationship: false
    Destination Volume Node: cluster2-node1
    Relationship ID: -
    Transfer Type: -
    Transfer Error: -
    Last Transfer Type: -
    Last Transfer Error: -
    Last Transfer Size: -
    Last Transfer Duration: -
    Last Transfer From: -
Last Transfer End Timestamp: -
```



---

```
Progress Last Updated: -  
Relationship Capability: Pre 8.2  
Lag Time: -  
SnapMirror Policy: -
```

2 entries were displayed.

## Restrictions/Limitations

The `snapmirror show` command will display values only for the following fields for relationships with "Relationship Capability" of "Pre 8.2", when run on the source cluster of a cross-cluster relationship: source-path, source-cluster, source-vserver, source-volume, destination-path, destination-cluster, destination-vserver, destination-volume, type, status, state, is-constituent, relationship-capability. You must issue the `snapmirror show` command on the destination cluster to have complete information about SnapMirror relationships.

For SnapMirror relationships between Infinite Volumes, the Total Progress, Snapshot Progress, Destination Volume Node, and Snapshot Checkpoint fields will not display values in the `snapmirror show` output.

If the SnapMirror relationship is between Infinite Volumes, and the Source Path field's value is `SRC_VOLUME_UNRESOLVED`, or the Destination Path field's value is `DST_VOLUME_UNRESOLVED`, check the intercluster connectivity for that relationship.

### See Also

`snapmirror list-destinations`

---

## snapmirror update-ls-set

Start an incremental load-sharing set transfer

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

### Description

The `snapmirror update-ls-set` command updates a set of load-sharing mirrors. The command makes destination volumes, in the group of load-sharing mirrors, up-to-date mirrors of the source volume.

The key parameter that identifies the set of load-sharing mirrors is the source volume. SnapMirror transfers are performed from the source volume to each of the up-to-date destination volumes in the set of load-sharing mirrors.

If the destination volume is empty, the `snapmirror update-ls-set` command performs a baseline transfer, that is, Data ONTAP takes a Snapshot copy on the source volume to capture the current image of the source volume and transfers all of the Snapshot copies on the source volume to each of the destination volumes. During a baseline transfer, the first Snapshot copy transferred becomes the temporary exported Snapshot copy on the destination volume. The exported Snapshot copy is the view to which clients are redirected on the destination volume while succeeding Snapshot copies are transferred.

If the destination volume is not empty, the `snapmirror update-ls-set` command performs an incremental transfer to each of the destination volumes. During an incremental transfer, Data ONTAP takes a Snapshot copy on the source volume to capture the current image of the source volume, finds the most recent common Snapshot copy between the source and destination volumes, and incrementally transfers Snapshot copies that are newer than the common Snapshot copy to the destination volume.

Note:

You still need to use the `snapmirror update-ls-set` command to manually update the set of load-sharing mirrors even if the set only has one destination mirror. The `snapmirror update` command can only be used to bring up to date a specific destination mirror that is lagging to the set.

---

After an update using the `snapmirror update-ls-set` command successfully completes, the last Snapshot copy transferred is made the new exported Snapshot copy on the destination volumes.

This command is not supported on Infinite Volume snapmirror relationships.

This command is only supported for SnapMirror relationships with the field "Relationship Capability" showing as "Pre 8.2" in the output of the `snapmirror show` command.

## Parameters

{ **-source-path** | **-S** {<[vserver:]volume>|<[cluster:][//vserver/]volume>} - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

| **-source-cluster** <cluster\_name> - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver** <vserver name> - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume** <volume name> } - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

[**-foreground** | **-w** [true]] - Foreground Process

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

---

To update the group of load-sharing mirrors for the source endpoint named `//vs1/dept_eng`, type the following command:

```
clus1::> snapmirror update-ls-set -source-path //vs1/dept_eng
```

## See Also

`snapmirror update`   `snapmirror show`

---

## snapmirror update

Start an incremental transfer

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

### Description

The `snapmirror update` command updates the destination volume of a SnapMirror relationship. The `snapmirror update` command behaves differently for data protection, vault, and load-sharing relationships. Refer to parameter "type" from `snapmirror create` to understand different types of relationships supported by SnapMirror.

The `snapmirror update` command performs an incremental transfer.

Before using this command, the relationship must be initialized using the `snapmirror initialize` or `snapmirror initialize-ls-set` commands.

For data protection relationships, the `snapmirror update` command makes the destination volume an up-to-date mirror of the source volume with the following steps:

- If the source volume is read-write, takes a Snapshot copy on the source volume to capture the current image of the source volume
- Finds the most recent Snapshot copy on the destination volume and validates that the corresponding Snapshot copy is on the source
- Incrementally transfers Snapshot copies that are newer than the corresponding Snapshot copy to the destination volume

You can use the `snapmirror update` command to update a specific load-sharing mirror that lags behind up-to-date destination volumes in the set of load-sharing mirrors. An update to the lagging load-sharing mirror should bring it up to date with the other up-to-date destination volumes in the set of load-sharing mirrors.

Note:

Using the `snapmirror update` command to update a set of load-sharing mirrors will not work. Use the `snapmirror update-ls-set` command to update a set of load-sharing mirrors.

For vault relationships, the `snapmirror update` does not take a Snapshot copy on the source volume but transfers only selected Snapshot copies that are newer than

---

the common Snapshot copy to the destination volume. Snapshot copies are selected by matching the value of `-snapmirror-label` of a Snapshot copy with the value of `-snapmirror-label` of one of the rules from the corresponding SnapMirror policy associated with the SnapMirror relationship. All matching Snapshot copies are incrementally transferred to the destination volume.

For vault relationships, the `snapmirror update` command also manages expiration of Snapshot copies on the destination volume. It does so by deleting Snapshot copies that have exceeded the value of `-keep` for the matching rule from the corresponding SnapMirror policy associated with the SnapMirror relationship. Snapshot copies that match the same `-snapmirror-label` will be deleted in oldest-first order.

For data protection relationships, the parameter `-source-snapshot` is optional and only allows for the transfer of Snapshot copies newer than the common Snapshot copy up to the specified `-source-snapshot`.

For vault relationships, the parameter `-source-snapshot` is optional and allows transfer of a Snapshot copy that is older than the common Snapshot copy and/or may not be selected for transfer based on policy-based selection of a scheduled update transfer.

After the `snapmirror update` command successfully completes, the last Snapshot copy transferred is made the new exported Snapshot copy on the destination volume. If an update to a vault relationship specifies a Snapshot copy using the `-source-snapshot` parameter that is older than the common snapshot, after the `snapmirror update` successfully completes, the exported Snapshot copy on the destination volume will remain unchanged.

If the `snapmirror update` does not finish successfully—for example, due to a network failure or because a `snapmirror abort` command was issued—a restart checkpoint might be recorded on the destination volume. If a restart checkpoint is recorded, the next update restarts and continues the transfer from the restart checkpoint. For vault relationships, the next update will restart and continue the old transfer regardless of whether it is a matching Snapshot copy or not.

If you add an aggregate to the source Infinite Volume, you must also add an aggregate of the same or greater size to the destination Infinite Volume before any `snapmirror update` occurs.

This command is supported for SnapMirror relationships with the field "Relationship Capability" showing as either "8.2 and above" or "Pre 8.2" in the output of the `snapmirror show` command.

For relationships with "Relationship Capability" of "8.2 and above", you can track the progress of the operation using the `snapmirror show` command.

For relationships with "Relationship Capability" of "Pre 8.2", a job will be spawned to operate on the SnapMirror relationship, and the job id will be shown in the command

---

output. The progress of the job can be tracked using the `job show` and `job history show` commands.

The `snapmirror update` command must be used from the destination Vserver or cluster.

## Parameters

**{ -source-path | -S {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Source Path

Specifies the source endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

**| -source-cluster <cluster\_name>** - Source Cluster

Specifies the source cluster of the SnapMirror relationship. If this parameter is specified, the `-source-vserver` and `-source-volume` parameters must also be specified. This parameter is only applicable for relationships with "Relationship Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-source-vserver <vserver name>** - Source Vserver

Specifies the source Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-source-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**-source-volume <volume name> }** - Source Volume

Specifies the source volume of the SnapMirror relationship. If this parameter is specified, parameters `-source-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-source-cluster` must also be specified.

**{ -destination-path {<[vserver:]volume>|<[cluster:][//vserver/]volume>}** - Destination Path

Specifies the destination endpoint of the SnapMirror relationship in one of two path formats. The normal format includes the names of the Vserver (vserver) and volume (volume). To support relationships with "Relationship Capability" of "Pre 8.2", a format which also includes the name of the cluster (cluster) is provided. The "Pre 8.2" format cannot be used when operating in a Vserver context.

**| -destination-cluster <cluster\_name>** - Destination Cluster

Specifies the destination cluster of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and `-destination-volume` must also be specified. This parameter is only applicable for relationships with "Relationship

---

Capability" of "Pre 8.2". This parameter cannot be specified when operating in a Vserver context.

**-destination-vserver** <vserver name> - Destination Vserver

Specifies the destination Vserver of the SnapMirror relationship. If this parameter is specified, parameters `-destination-volume` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**-destination-volume** <volume name> } - Destination Volume

Specifies the destination volume of the SnapMirror relationship. If this parameter is specified, parameters `-destination-vserver` and for relationships with "Relationship Capability" of "Pre 8.2", `-destination-cluster` must also be specified.

**[-source-snapshot | -s <text>]** - Source Snapshot

This optional parameter specifies a Snapshot copy to transfer. The default behavior, in many cases, is that Data ONTAP creates a new Snapshot copy and uses it as the basis for determining what data are replicated; with this option, the specified Snapshot copy will be used instead. For vault relationships, the specified Snapshot copy may be newer or older than the common Snapshot copy; for data protection relationships, the specified Snapshot copy must be newer than the latest common Snapshot copy. This parameter is not supported for relationships with "Relationship Capability" of "Pre 8.2".

**[-throttle | -k <throttleType>]** - Throttle (KB/sec)

This optional parameter limits the network bandwidth used for the update transfer when the source and destination endpoints belong to different clusters. It sets the maximum rate (in Kbytes/sec) at which data can be transferred between the clusters during the operation. If this parameter is not specified, the throttle value configured for the relationship with the `snapmirror create` or `snapmirror modify` commands will be used. To specify fully using the network bandwidth available between the clusters, set the throttle value to unlimited or 0. The minimum throttle value is four Kbytes/sec, so if you specify a throttle value between 1 and 4, it will be treated as if you specified 4. The `-throttle` option does not affect load-sharing transfers and other transfers confined to a single cluster.

**[-transfer-priority {low|normal}]** - Transfer Priority

This optional parameter specifies the priority at which the transfer runs. The default value for this parameter is the value in the SnapMirror policy associated with this relationship. This parameter is not applicable to relationships with a "Relationship Capability" of "Pre 8.2".

**[-foreground | -w [true]]** - Foreground Process



---

This specifies whether the operation runs as a foreground process. If this parameter is specified, the default setting is true (the operation runs in the foreground). When set to true, the command will not return until the process completes. This parameter is only applicable to relationships with "Relationship Capability" of "Pre 8.2".

## Examples

To update the mirror relationship between the destination endpoint vs2:dept\_eng\_dp\_mirror3 and its source endpoint, type the following command:

```
vs2::> snapmirror update -destination-path  
vs2:dept_eng_dp_mirror3
```

For relationships with "Relationship Capability" of "Pre 8.2", to update the mirror relationship between the destination endpoint clus2://vs2/dept\_eng\_dp\_mirror3 and its source endpoint, type the following command:

```
clus2::> snapmirror update -destination-path  
clus2://vs2/dept_eng_dp_mirror3
```

## See Also

snapmirror create snapmirror modify snapmirror initialize snapmirror initialize-  
ls-set snapmirror update-ls-set snapmirror abort snapmirror show job show  
job history show snapmirror policy

---

## snapmirror policy add-rule

Add a new rule to SnapMirror policy

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

### Description

The `snapmirror policy add-rule` command adds a rule to a SnapMirror policy. Rules define which Snapshot copies are protected by vault relationships. A rule must not be added to a policy that will be associated with a SnapMirror data protection relationship. A policy that will be associated with a SnapMirror vault relationship must have at least one rule. A SnapMirror policy can have at most 10 rules.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

This parameter specifies the SnapMirror policy name.

**-snapmirror-label** <text> - Snapshot Copy Label

This parameter is used for the purpose of Snapshot copy selection as well as for accounting of Snapshot copies at the SnapMirror vault destination. Only Snapshot copies that have a SnapMirror label that matches this parameter will be transferred to the SnapMirror vault destination. The label can be 31 or fewer characters in length.

**-keep** <text> - Snapshot Copy Retention Count

This parameter specifies the maximum number of Snapshot copies that are retained on the SnapMirror vault destination volume for a rule. The total number of Snapshot copies retained for all the rules in a policy cannot exceed 251.

**[-preserve {true|false}]** - Snapshot Copy Preserve Enabled

This parameter specifies the behavior when the Snapshot copy retention count is reached on the SnapMirror vault destination for the rule. The default value is `false`, which means that the oldest Snapshot copy will be rotated out to make room for new ones only if the number of Snapshot copies has exceeded the retention count specified in the "keep" parameter. When set to `true`, an incremental SnapMirror vault update will fail when the Snapshot copies have reached the retention count.

---

**[-warn <integer>]** - Warning Threshold Count

This parameter specifies the warning threshold count for the rule. The default value is 0. When set to a value greater than zero, an event is generated after the remaining number of Snapshot copies (for the particular rule) retained on a SnapMirror vault destination reaches the specified warn limit. The preserve parameter for the rule must be true to set the warn parameter to a value greater than zero.

## Examples

The following example adds a rule named `nightly` to the SnapMirror policy named `TieredBackup` on Vserver `vs0`. The rule will retain a maximum of 5 nightly Snapshot copies.

```
vs0::> snapmirror policy add-rule -vserver vs0 -policy TieredBackup -snapmirror-label nightly -keep 5
```

## snapmirror policy create

Create a new SnapMirror policy

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

## Description

The `snapmirror policy create` command creates a SnapMirror policy. When applied to a SnapMirror relationship, the SnapMirror policy specifies the configuration attributes for that relationship. The default policies `DPDefault` and `XDPDefault` are created by the system.

For vault relationships, policies have rules that define which Snapshot copies are protected.

Note:

Use the `snapmirror policy add-rule` command to add a rule to a policy.

## Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

---

This parameter specifies the SnapMirror policy name. A policy name can be made up of the characters A to Z, a to z, 0 to 9, ".", "-", and "\_". The name can be up to 256 characters in length.

**[-comment <text>]** - Comment

This parameter specifies a text comment for the SnapMirror policy. If the comment contains spaces, it must be enclosed within quotes.

**[-tries <unsigned32\_or\_unlimited>]** - Tries Limit

This parameter determines the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The value of this parameter must be a positive integer or unlimited. The default value is 8.

**[-transfer-priority {low|normal}]** - Transfer Scheduling Priority

This parameter specifies the priority at which a transfer runs. The supported values are normal or low. The normal transfers are scheduled before the low priority transfers. The default is normal.

**[-ignore-atime {true|false}]** - Ignore File Access Time

This parameter applies only to vault relationships. It specifies whether incremental transfers will ignore files which have only their access time changed. The supported values are true or false. The default is false.

**[-restart {always|never|default}]** - Restart Behavior

This parameter applies only to data protection relationships. It defines the behavior of SnapMirror if an interrupted transfer exists. The supported values are always, never, or default. If the value is set to always, an interrupted SnapMirror transfer always restarts provided it has a restart checkpoint and the conditions are the same as they were before the transfer was interrupted. In addition, a new SnapMirror Snapshot copy is created which will then be transferred. If the value is set to never, an interrupted SnapMirror transfer will never restart, even if a restart checkpoint exists. A new SnapMirror Snapshot copy will still be created and transferred. Data ONTAP version 8.2 will interpret a value of default as being the same as always. Vault transfers will always resume based on a restart checkpoint, provided the Snapshot copy still exists on the source volume.

## Examples

The following example creates a SnapMirror policy named TieredBackup on a Vserver named vs0.

```
vs0::> snapmirror policy create -vserver vs0 -policy TieredBackup -tries 10 -  
restart never
```

---

## See Also

snapmirror policy add-rule

---

## snapmirror policy delete

Delete a SnapMirror policy

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

### Description

The `snapmirror policy delete` command deletes a SnapMirror policy. A policy that is to be deleted must not be associated with any SnapMirror relationship. The default policies `DPDefault` and `XDPDefault` cannot be deleted.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

This parameter specifies the SnapMirror policy name.

### Examples

The following example deletes a SnapMirror policy named `TieredBackup` on Vserver `vs0`:

```
vs0::> snapmirror policy delete -vserver vs0 -policy TieredBackup
```

## snapmirror policy modify-rule

Modify an existing rule in SnapMirror policy

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

### Description

The `snapmirror policy modify-rule` command can be used to modify the retention count, preserve setting, and warning threshold count for a rule in a SnapMirror policy. Reducing the retention count or disabling the preserve setting for a rule in a SnapMirror policy might result in the deletion of Snapshot copies on the vault destination when the next transfer by the `snapmirror update` command occurs.

---

## Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

This parameter specifies the SnapMirror policy name.

**-snapmirror-label** <text> - Snapshot Copy Label

This parameter specifies the rule that is to be modified in a SnapMirror policy.

**[-keep <text>]** - Snapshot Copy Retention Count

This parameter specifies the maximum number of Snapshot copies that are retained on the SnapMirror vault destination volume for a rule. The total number of Snapshot copies retained for all the rules in a policy cannot exceed 251.

**[-preserve {true|false}]** - Snapshot Copy Preserve Enabled

This parameter specifies the behavior when the Snapshot copy retention count is reached on the SnapMirror vault destination for the rule. The default value is false, which means that the oldest Snapshot copy will be rotated out to make room for new ones only if the number of Snapshot copies has exceeded the retention count specified in the "keep" parameter. When set to true, an incremental SnapMirror vault update will fail when the Snapshot copies have reached the retention count.

**[-warn <integer>]** - Warning Threshold Count

This parameter specifies the warning threshold count for the rule. The default value is 0. When set to a value greater than zero, an event is generated after the remaining number of Snapshot copies (for the particular rule) retained on a SnapMirror vault destination reaches the specified warn limit. The preserve parameter for the rule must be true to set the warn parameter to a value greater than zero.

## Examples

The following example changes the retention count for nightly Snapshot copies to 6 for a rule named nightly on a SnapMirror policy named TieredBackup on Vserver vs0:

```
vs0::> snapmirror policy modify-rule -vserver vs0 -policy TieredBackup -  
snapmirror-label nightly -keep 6
```

## See Also

snapmirror update

---

## snapmirror policy modify

Modify a SnapMirror policy

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

### Description

The `snapmirror policy modify` command can be used to modify the policy attributes.

Note:

Use the `snapmirror policy modify-rule` command to modify a rule in a SnapMirror policy.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

This parameter specifies the SnapMirror policy name.

**[-comment** <text>] - Comment

This parameter specifies a text comment for the SnapMirror policy. If the comment contains spaces, it must be enclosed within quotes.

**[-tries** <unsigned32\_or\_unlimited>] - Tries Limit

This parameter determines the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The value of this parameter must be a positive integer or unlimited. The default value is 8.

**[-transfer-priority** {low|normal}] - Transfer Scheduling Priority

This parameter specifies the priority at which a transfer runs. The supported values are normal or low. The normal transfers are scheduled before the low priority transfers. The default is normal.

**[-ignore-atime** {true|false}] - Ignore File Access Time



---

This parameter applies only to vault relationships. It specifies whether incremental transfers will ignore files which have only their access time changed. The supported values are true or false. The default is false.

**[-restart {always|never|default}]** - Restart Behavior

This parameter applies only to data protection relationships. It defines the behavior of SnapMirror if an interrupted transfer exists. The supported values are always, never, or default. If the value is set to always, an interrupted SnapMirror transfer always restarts provided it has a restart checkpoint and the conditions are the same as they were before the transfer was interrupted. In addition, a new SnapMirror Snapshot copy is created which will then be transferred. If the value is set to never, an interrupted SnapMirror transfer will never restart, even if a restart checkpoint exists. A new SnapMirror Snapshot copy will still be created and transferred. Data ONTAP version 8.2 will interpret a value of default as being the same as always. Vault transfers will always resume based on a restart checkpoint, provided the Snapshot copy still exists on the source volume.

## Examples

The following example changes the "transfer-priority" and the "comment" text of a snapmirror policy named TieredBackup on Vserver vs0:

```
vs0::> snapmirror policy modify -vserver vs0 -policy TieredBackup -transfer-  
priority low -comment "Use for tiered backups"
```

## See Also

snapmirror policy modify-rule

---

## snapmirror policy remove-rule

Remove a rule from SnapMirror policy

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

### Description

The `snapmirror policy remove-rule` command removes a rule from a SnapMirror policy. On the vault destination, all Snapshot copies with a SnapMirror label matching the rule are no longer processed by the `snapmirror update` command and might need to be deleted manually. A SnapMirror policy associated with a SnapMirror vault relationship must have at least one rule.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver for the SnapMirror policy.

**-policy** <sm\_policy> - SnapMirror Policy Name

This parameter specifies the SnapMirror policy name.

**-snapmirror-label** <text> - Snapshot Copy Label

This parameter specifies the rule that is removed from the SnapMirror policy.

### Examples

The following example removes a rule named `nightly` from a SnapMirror policy named `TieredBackup` on Vserver `vs0`:

```
vs0::> snapmirror policy remove-rule -vserver vs0 -policy TieredBackup -  
snapmirror-label nightly
```

### See Also

`snapmirror update`

---

## snapmirror policy show

Show SnapMirror policies

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

### Description

The `snapmirror policy show` command displays the following information about SnapMirror policies:

- Vserver Name
- SnapMirror Policy Name
- Number of Rules in the policy
- Tries
- Transfer Priority
- Restart
- Comment for the policy
- Individual Rule Names
- Keep value for the Rule

### Parameters

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

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

| [-**instance** ] }

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

[-**vserver** <vserver name>] - Vserver Name

Selects the policies that match this parameter value.

[-**policy** <sm\_policy>] - SnapMirror Policy Name

---

Selects the policies that match this parameter value.

**[-owner {cluster-admin|vserver-admin}]** - Owner of the Policy

Selects the policies that match this parameter value. A policy can be owned by either the "Cluster Admin" or a "Vserver Admin".

**[-comment <text>]** - Comment

Selects the policies that match this parameter value.

**[-tries <unsigned32\_or\_unlimited>]** - Tries Limit

Selects the policies that match this parameter value.

**[-transfer-priority {low|normal}]** - Transfer Scheduling Priority

Selects the policies that match this parameter value.

**[-ignore-atime {true|false}]** - Ignore File Access Time

Selects the policies that match this parameter value.

**[-restart {always|never|default}]** - Restart Behavior

Selects the policies that match this parameter value.

**[-snapmirror-label <text>, ...]** - Snapshot Copy Label

Selects the policies that match this parameter value.

**[-keep <text>, ...]** - Snapshot Copy Retention Count

Selects the policies that match this parameter value.

**[-preserve {true|false}, ...]** - Snapshot Copy Preserve Enabled

Selects the policies that match this parameter value.

**[-warn <integer>, ...]** - Warning Threshold Count

Selects the policies that match this parameter value.

**[-total-rules <integer>]** - Total Rules in the Policy

Selects the policies that match this parameter value.

**[-total-keep <integer>]** - Total Retention Count for All Rules in the Policy

Selects the policies that match this parameter value.

## Examples

The following example displays information about all SnapMirror policies:

```
cs::> snapmirror policy show
```

---

Vserver Name	Policy Name	Number Of Rules	Tries	Transfer Priority	Restart	Comment
cs	DPDefault	0	8	normal	always	Default policy
	for DP relationship.					
	Snapmirror-label: -					
				Total	Keep:	-
					Keep:	0
cs	XDPDefault	2	8	normal	always	Default policy
	for XDP relationship with daily and weekly rules.					
	Snapmirror-label: daily				Keep:	7
	weekly					52
				Total	Keep:	59
vs0	TieredBackup	0	8	normal	always	Use for tiered
	backups					
	Snapmirror-label: -					
				Total	Keep:	-
					Keep:	0

3 entries were displayed.

The following example shows all the policies with the following fields - vserver (default), policy (default) and transfer-priority:

```
cs::> snapmirror policy show -fields transfer-priority
vserver      policy      transfer-priority
-----
cs           DPDefault  normal
cs           XDPDefault
vs0          TieredBackup
              normal
3 entries were displayed.
```

---

## snapmirror snapshot-owner create

Add an owner to preserve a Snapshot copy for a SnapMirror mirror-to-vault cascade configuration

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

### Description

The `snapmirror snapshot-owner create` command adds an owner to the specified Snapshot copy. An owner is used to prevent premature deletion of a Snapshot copy from the primary volume in a SnapMirror mirror-to-vault cascade configuration. A Snapshot copy can have at most one owner. An owner can only be added to a Snapshot copy on a read-write volume. The Snapshot copy must have a valid SnapMirror label that was added using the `volume snapshot create` or the `volume snapshot modify` command.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume.

**-snapshot** <snapshot name> - Snapshot Copy Name

This parameter specifies the name of the Snapshot copy.

**[-owner** <owner name>] - Snapshot Copy Owner Name

This parameter specifies the name of the owner for the Snapshot copy. The owner name can be made up of the characters A to Z, a to z, 0 to 9, and "\_". The name can be up to 32 characters in length. When not specified, an owner will be added with a system-generated default name.

### Examples

The following example adds owner `app1` on Snapshot copy `snap1` on volume `vol1` in Vserver `vs0`.

```
clus1:>> snapmirror snapshot-owner create -vserver vs0 -volume vol1 -snapshot  
snap1 -owner appl
```

---

The following example adds a default owner on Snapshot copy snap2 on volume vol1 in Vserver vs0.

```
clus1::> snapmirror snapshot-owner create -vserver vs0 -volume vol1 -snapshot  
snap2
```

## See Also

volume snapshot create   volume snapshot modify

---

## snapmirror snapshot-owner delete

Delete an owner used to preserve a Snapshot copy for a SnapMirror mirror-to-vault cascade configuration

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

### Description

The `snapmirror snapshot-owner delete` command removes an owner on the specified Snapshot copy, that was added using the `snapmirror snapshot-owner create` command.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume.

**-snapshot** <snapshot name> - Snapshot Copy Name

This parameter specifies the name of the Snapshot copy.

**[-owner <owner name>]** - Snapshot Copy Owner Name

This parameter specifies the name of the owner for the Snapshot copy. When not specified, the owner with the system-generated default name will be removed.

### Examples

The following example removes owner `app1` on Snapshot copy `snap1` on volume `vol1` in Vserver `vs0`.

```
clus1:> snapmirror snapshot-owner delete -vserver vs0 -volume vol1 -snapshot  
snap1 -owner appl
```

The following example removes the default owner on Snapshot copy `snap2` on volume `vol1` in Vserver `vs0`.

```
clus1:> snapmirror snapshot-owner delete -vserver vs0 -volume vol1 -snapshot  
snap2
```

### See Also



---

snapmirror snapshot-owner create

---

# snapmirror snapshot-owner show

Display Snapshot copies with owners

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

## Description

The `snapmirror snapshot-owner show` command lists all Snapshot copies with owners that were added using the `snapmirror snapshot-owner create` command.

## Parameters

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

If this parameter is specified, the command displays information about the specified fields.

| [-instance ] }

If this parameter is specified, the command displays detailed information about all fields.

**-vserver** <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume.

**[-snapshot** <snapshot name>] - Snapshot Copy Name

If this parameter is specified, the command displays the owner name for the specified Snapshot copy.

## Examples

The following example lists all Snapshot copies with owners on volume vol1 in Vserver vs0. The system-generated default owner name is displayed as "-".

```
clus1:>> snapmirror snapshot-owner show -vserver vs0 -volume vol1
Vserver Volume Snapshot Owner Names
-----
vs0      vol1      snap2      -
          snap1      snap1      appl
```

The following example displays the owner name for Snapshot copy snap1 on volume vol1 in Vserver vs0.

---

```
clus1:> snapmirror snapshot-owner show -vserver vs0 -volume vol1 -snapshot snap1
  Vserver: vs0
  Volume: vol1
  Snapshot: snap1
  Owner Names: appl
```

## See Also

`snapmirror snapshot-owner create`

---

## statistics show-periodic

Continuously display current performance data at regular intervals

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

### Description

This command continuously displays specified performance data at regular intervals. The command output displays data in the following columns:

- **cpu busy:** Overall system utilization based on CPU utilization and subsystem utilization. Examples of subsystems include the storage subsystem and RAID subsystem.
- **total ops:** The number of total operations per second.
- **nfs-ops:** The number of NFS operations per second.
- **cifs-ops:** The number of CIFS operations per second.
- **data busy:** The percentage of time that data ports sent or received data.
- **data recv:** Network traffic received on data ports (KBps).
- **data sent:** Network traffic sent on data ports (KBps).
- **cluster busy:** The percentage of time that cluster ports sent or received data.
- **cluster recv:** Network traffic received on cluster ports (KBps).
- **cluster sent:** Network traffic sent on cluster ports (KBps).
- **disk read:** Data read from disk (KBps).
- **disk write:** Data written to disk (KBps).

### Parameters

**-object <text>** - Object

Selects the object for which you want to display performance data. The default object is "cluster".

**-instance <text>** - Instance

Selects the instance for which you want to display performance data. This parameter is required if you specify the `-object` parameter and enter any object other than "cluster".

For example, if you want to display disk object statistics, you can use this parameter to specify the name of a specific disk whose statistics you want to view.

**-counter** <text> - Counter

Selects the counters for which you want to display performance data. If you do not specify this parameter, the command displays statistics for all of the counters in the specified objects.

**-node** {<nodename>|local} - Node

Selects the nodes for which you want to display performance data. The default node is "cluster:summary".

**-vserver** <vserver name> - Vserver

Selects the Vserver for which you want to display performance data. If you do not specify this parameter, the command displays statistics for all of the Vservers in the cluster.

**-interval** <integer> - Interval in Seconds

Specifies, in seconds, the interval between statistics updates. The default setting is 1 second.

**-iterations** <integer> - Number of Iterations

Specifies the number of iterations the command runs before terminating. The default setting is 0 (zero); this means that the command continues to run until you interrupt it by pressing Ctrl-C.

**-summary** {true|false} - Print Summary

Specifies whether the command prints a final summary of statistics after the command has gone through all of its iterations. The default setting is `true`.

**[-filter** <text>] - Filter Data (privilege: advanced)

Selects instances that match the specified filter criteria. For example, to display instances from node1, specify `-filter "node_name=node1"`.

## Examples

The following example displays the "cluster" statistics for a node named node1. Because no number of iterations is specified, this command will continue to run until you interrupt it by pressing Ctrl-C.

```
cluster1::> statistics show-periodic -node node1
  cpu    total    disk    data    data    data cluster  cluster  cluster
  busy   ops    nfs-ops cifs-ops busy    recv    sent    busy    recv    sent
  read   write
-----
-----
```

54%	10378	10378	0	59%	66.9MB	99.6MB	72%	78.8MB	172MB
8.25KB	24.7KB								
49%	8156	8156	0	47%	48.0MB	82.0MB	79%	83.9MB	190MB
7.92KB	7.92KB								
49%	6000	6000	0	54%	24.3MB	87.0MB	76%	109MB	182MB
15.8KB	0B								
56%	10363	10363	0	71%	62.3MB	110MB	57%	96.8MB	136MB
8.00KB	24.0KB								
54%	10460	10460	0	66%	65.8MB	106MB	59%	94.7MB	141MB
0B	0B								
54%	7894	7894	0	62%	40.1MB	101MB	78%	99.0MB	186MB
2.68MB	11.0MB								
56%	7135	7135	0	65%	30.5MB	104MB	86%	93.3MB	206MB
16.2KB	32.3KB								
60%	11374	11374	0	78%	67.7MB	126MB	87%	88.5MB	209MB
0B	0B								
56%	10458	10458	0	72%	65.7MB	112MB	86%	87.1MB	205MB
16.0KB	0B								
56%	10130	10130	0	59%	64.9MB	98.9MB	84%	81.0MB	200MB
8.00KB	24.0KB								
55%	9814	9814	0	52%	63.8MB	76.4MB	94%	71.2MB	224MB
0B	0B								
54%	7776	7776	0	49%	41.2MB	80.7MB	91%	86.4MB	218MB
24.5KB	8.16KB								
52%	7400	7400	0	49%	38.0MB	80.8MB	87%	98.7MB	208MB
7.92KB	23.8KB								
55%	9459	9459	0	65%	56.4MB	105MB	65%	96.6MB	155MB
0B	0B								
56%	10529	10529	0	65%	65.8MB	107MB	69%	89.0MB	165MB
16.2KB	0B								
57%	9950	9950	0	62%	64.9MB	95.3MB	89%	81.8MB	213MB
2.32MB	2.65MB								
54%	8287	8287	0	48%	51.9MB	77.2MB	95%	73.3MB	226MB
8.16KB	8.16KB								
54%	7612	7612	0	40%	41.4MB	68.2MB	95%	88.6MB	228MB
15.8KB	0B								
54%	8728	8728	0	60%	48.9MB	92.8MB	89%	103MB	214MB
7.92KB	23.8KB								
57%	9944	9944	0	70%	59.4MB	108MB	74%	95.7MB	176MB
0B	0B								

[...]

The following example displays the "processor" statistics for an instance named processor1. This command will display only five iterations.

```
cluster1::> statistics show-periodic -object processor -instance processor1 -
iteration 5
instance      node processor      elapsed      sk
name          name      busy      time switches
-----
processor0    -          2%          -          1022
processor0    -          1%          -           959
processor0    -          2%          -          1098
processor0    -          2%          -           870
processor0    -          2%          -          1107
[...]
```

---

## statistics show

Display performance data for a time interval

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

### Description

Attention:

This command will be changed from the administrative privilege level to the diagnostic privilege level in a future major release.

This command displays performance data for a period of time.

To display data for a period of time, collect a sample using the `statistics start` and `statistics stop` commands. The data that displays is calculated data based on the samples the cluster collects. To view the sample, specify the `-sample-id` parameter.

### Parameters

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

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

**[-object <text>]** - Object

Selects the objects for which you want to display performance data. To view a list of valid object names, type `statistics show -object ?` or `statistics catalog object show`.

Caution:

You should limit the scope of this command to only a few objects at a time to avoid a potentially significant impact on the performance of the system.

**[-instance <text>]** - Instance

Selects the instances for which you want to display performance data. If you do not specify this parameter, the command displays statistics for all of the instances associated with the specified objects.

---

For example, if you want to display disk object statistics, you can use this parameter to specify the name of a specific disk whose statistics you want to view. If you do not specify this parameter, the command displays statistics for all disks in the system.

**[-counter <text>]** - Counter

Selects the counters for which you want to display performance data.

**[-node {<nodename>|local}]** - Node

Selects the nodes for which you want to display performance data.

**[-vserver <vserver name>]** - Vserver

Selects the Vserver for which you want to display performance data.

**[-value <Counter64>]** - Value (privilege: advanced)

Selects the performance data that matches the specified counter value.

**[-labels <text>, ...]** - List of Labels (privilege: advanced)

Selects the performance data that matches the specified label.

**[-values <text>, ...]** - List of Values (privilege: advanced)

Displays only the statistics that have the specified values.

**[-filter <text>]** - Filter Data (privilege: advanced)

Selects performance data for the instance that matches the specified filter criteria. For example, to display the instances that match a value of greater than 50 for the total\_ops counter, specify `-filter "total_ops>50"`.

**[-sample-id <text>]** - Sample Identifier

Displays performance data for the specified sample. You collect a sample by using the statistics start and statistics stop commands.

## Examples

The following example displays the statistics that were collected for sample "smp1\_1":

```
cluster1::> statistics show -sample-id smp1_1
Object: system
Instance: system
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
```

Counter	Value
avg_processor_busy	6%
cifs_ops	0
cpu_busy	6%
disk_data_read	0B
disk_data_written	0B
fcp_data_recv	0B
fcp_data_sent	0B
fcp_ops	0



---

```
hdd_data_read          0B
hdd_data_written       0B
hostname               node-name1
http_ops               0
instance_name          system
iscsi_ops               0
net_data_recv          88.0KB
net_data_sent          5.00KB
nfs_ops                0
node_name              node-name1
node_uuid
[...]
```

## See Also

`statistics catalog object show` `statistics start` `statistics stop`

---

## statistics start

Start data collection for a sample

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

### Description

Attention:

This command will be changed from the administrative privilege level to the diagnostic privilege level in a future major release.

This command starts the collection of performance data. Use the `statistics stop` command to stop the collection. You view the sample of performance data by using the `statistics show` command. You can collect more than one sample at a time.

### Parameters

**-object <text>** - Object

Selects the objects for which you want to collect performance data. This parameter is required. To view a list of valid object names, type `statistics catalog object show` at the command prompt.

Caution:

You should limit the scope of this command to only a few objects at a time to avoid a potentially significant impact on the performance of the system.

**[-instance <text>]** - Instance

Selects the instances for which you want to collect performance data. If you do not specify this parameter, the command collects statistics for all of the instances associated with the specified objects.

For example, if you want to collect disk object statistics, you can use this parameter to specify the name of a specific disk whose statistics you want to view. If you do not specify this parameter, the command will collect statistics for all disks in the system.

**[-counter <text>]** - Counter

---

Selects the counters for which you want to collect performance data. If you do not specify this parameter, the command collects statistics for all of the counters in the specified objects.

**[-sample-id <text>]** - Sample Identifier

Specifies an identifier for the sample. Identifiers must be unique and are restricted to the characters 0-9, a-z, A-Z, and "\_". If you do not specify this parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. When you run the `statistics show` command without specifying the `-sample-id` parameter, data from the default sample displays. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous sample. The command does not delete the default sample when you close your session.

**[-vserver <vserver name>]** - Vserver

Selects the vservers for which you want to collect performance data. If you do not specify this parameter, the command collects statistics for all of the Vservers in the cluster.

**[-node {<nodename>|local}]** - Node

Selects the node for which you want to collect performance data. If you do not specify this parameter, the command collects statistics for all of the nodes in the cluster.

**[-filter <text>]** - Filter (privilege: advanced)

Selects performance data for the instance that matches the specified filter criteria. For example, to display the instances from node1, specify `-filter "node_name=node1"`.

## Examples

The following example starts statistics collection for sample "smp1\_1":

```
cluster1::> statistics start -object system -sample-id smp1_1
Statistics collection is being started for Sample-id: smp1_1
```

## See Also

`statistics catalog object show`   `statistics show`   `statistics stop`

---

## statistics stop

Stop data collection for a sample

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

### Description

Attention:

This command will be changed from the administrative privilege level to the diagnostic privilege level in a future major release.

This command stops the collection of performance data. You view the sample of performance data by using the `statistics show` command.

### Parameters

**[-sample-id <text>]** - Sample Identifier

Specifies the identifier of the sample for which you want to stop data collection. If you do not specify this parameter, the command stops data collection for the last sample that you started by running the `statistics start` command without the `-sample-id` parameter.

### Examples

The following example stops data collection for sample "smpl\_1":

```
cluster1::> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1
```

### See Also

`statistics start`   `statistics show`

---

## statistics catalog counter show

Display the list of counters in an object

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

### Description

This command displays the names and descriptions of counters. The displayed data is either node-specific or cluster-wide, depending on the objects specified.

### Parameters

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

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

| [-describe ] }

Displays detailed information about each counter, including privilege level, label, and whether the counter is a key counter.

[-object <text>] - Object

Selects the object for which you want to display the list of counters. This parameter is required. To view a list of valid object names, type `statistics catalog counter show -object ?` or `statistics catalog object show`.

[-counter <text>] - Counter

Selects the counters that match this parameter value. If you do not specify this parameter, the command displays details for all counters.

[-filter <text>] - Filter Data

Selects the counters that match this parameter value. For example, to display counters from node1, specify `-filter "node_name=node1"`.

[-label <text>, ...] - Labels for Array Counters

Selects the counters that match this parameter value. A label is the name of the bucket to which an array counter belongs.

[-description <text>] - Description

---

Selects the counters that match this parameter value.

**[-privilege <text>]** - Privilege Level (privilege: advanced)

Selects the counters that match this parameter value.

**[-is-key-counter {true|false}]** - Is Key Counter

Selects the counters that are key counters (true) or are not key counters (false). A key counter is a counter that uniquely identifies an instance across the cluster. The default setting is false. For example, "vserver\_name" and "node\_name" are key counters because they identify the specific Vserver or node to which the instance belongs.

### Examples

The following example displays the list of counters in the processor object.

```
cluster1::> statistics catalog counter show -object processor
Object: processor
Counter      Description
-----
instance_name Instance Name
instance_uuid Instance UUID
node_name    System node name
node_uuid    System node id
process_name  Ontap process that provided this instance
processor_busy Percentage of elapsed time that the processor
               is executing non-idle processes
processor_elapsed_time Wall-clock time since boot used for
               calculating processor utilization
sk_switches    Number of sk switches per second
8 entries were displayed.
```

### See Also

statistics catalog object show

---

## statistics catalog instance show

Display the list of instances associated with an object

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

### Description

This command displays the names of instances associated with the specified object. The displayed data is either node-specific or cluster-wide, depending on the objects specified.

### Parameters

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

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

**[-object <text>]** - Object

Selects the object for which you want to display the list of instances. This parameter is required. To view a list of valid object names, type `statistics catalog instance show -object ?` or `statistics catalog object show`.

**[-instance <text>]** - Instance Name

Selects the instances that match this parameter value. If you do not specify this parameter, the command displays all the instances.

**[-filter <text>]** - Filter Data

Selects the instances that match this parameter value. For example, to display instances from `vserver1`, specify `-filter "vserver_name=vserver1"`.

**[-vserver <vserver name>, ...]** - Vserver Name

Selects the instances that match this parameter value. If you do not specify this parameter, the command displays instances for all of the Vservers in the cluster.

**[-node {<nodename>|local}, ...]** - Node Name

Selects the instances that match this parameter value. If you do not specify this parameter, the command displays instances for all of the nodes in the cluster.

---

## Examples

The following example displays the list of instances associated with the processor object.

```
cluster1::> statistics catalog instance show -object processor
Object: processor
processor0
processor0
processor1
processor1
4 entries were displayed.
```

## See Also

`statistics catalog object show`



---

## statistics catalog object show

Display the list of objects

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

### Description

This command displays the names and descriptions of objects from which you can obtain performance data. The displayed data is either node-specific or cluster-wide, depending on the objects specified.

### Parameters

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

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

| [-**describe** ] }

Displays detailed information about each object, including privilege level.

[-**object** <text>] - Object

Selects the objects for which you want to display information. If you do not specify this parameter, the command displays details for all of the objects.

[-**privilege** <text>] - Privilege Level (privilege: advanced)

Selects the objects that match this parameter value.

[-**description** <text>] - Description

Selects the objects that match this parameter value.

### Examples

The following example displays descriptions of all objects in the cluster:

```
cluster1::> statistics catalog object show
aggregate          CM object for exporting aggregate performance
                   counters
audit_ng           CM object for exporting audit_ng performance
                   counters
avoa               Counter Manager (CM) object for exporting
                   antivirus on-access (AVOA) counters.
cifs               These counters report activity from both SMB
                   and SMB2 revisions of the CIFS protocol. For
                   information isolated to SMB, see the 'smb1'
```

---

cifs:node	object. For SMB2, see the 'smb2' object. These counters report activity from both SMB and SMB2 revisions of the CIFS protocol. For information isolated to SMB, see the 'smb1' object. For SMB2, see the 'smb2' object.
cifs:vserver	These counters report activity from both SMB and SMB2 revisions of the CIFS protocol. For information isolated to SMB, see the 'smb1' object. For SMB2, see the 'smb2' object.
cluster_peer	The cluster peer object contains peer counters.
[...]	

---

## statistics oncrpc show-replay-cache

Display ONC RPC ReplayCache Statistics

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

### Description

Attention:

This command is deprecated and will be removed in a future major release.

The `statistics oncrpc show-replay-cache` command displays information about the contents of the Open Network Computing Remote Procedure Call (ONC RPC) replay caches for the nodes of a cluster.

### Parameters

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

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

| **[-instance ]** }

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

**[-node {<nodename>|local}]** - Node

Use this parameter to display information only about the replay cache of the node you specify.

**[-protocol {TCP|UDP}]** - Protocol

Use this parameter to display information only about the replay caches for the network protocol you specify.

**[-in-prog-hits <Counter with Delta>]** - In Progress Hits

Use this parameter to display information only about the replay caches that contain the number of in-progress hits you specify.

**[-cache-hits <Counter with Delta>]** - Cache Hits

Use this parameter to display information only about the replay caches that contain the number of cache hits you specify.

**[-cache-misses <Counter with Delta>] - Cache Misses**

Use this parameter to display information only about the replay caches that contain the number of cache misses you specify.

**Examples**

The following example shows output for a cluster with two nodes.

```
cluster1::> statistics oncrpc show-replay-cache

Node      Value      Delta
node1
InProgress Hits: 0 -
Cache Hits: 0 -
Cache Misses: 0 -

Node      Value      Delta
node1
InProgress Hits: 0 -
Cache Hits: 0 -
Cache Misses: 0 -

Node      Value      Delta
node2
InProgress Hits: 0 -
Cache Hits: 0 -
Cache Misses: 0 -

Node      Value      Delta
node2
InProgress Hits: 0 -
Cache Hits: 0 -
Cache Misses: 0 -
4 entries were displayed.
```

---

## statistics oncrpc show-rpc-calls

Display ONC RPC Call Statistics

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

### Description

Attention:

This command is deprecated and will be removed in a future major release.

The `statistics oncrpc show-rpc-calls` command displays information about the Open Network Computing Remote Procedure Call (ONC RPC) calls performed by the nodes of a cluster.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Use this parameter to display information only about the RPC calls performed by the node you specify.

[-**protocol** {TCP|UDP}] - Transport Protocol

Use this parameter to display information only about the RPC calls performed using the network protocol you specify.

[-**badproc** <Counter with Delta>] - Bad Procedure Calls

Use this parameter to display information only about the RPC calls that have the number of bad procedure calls you specify. Bad procedure calls are RPC requests that contain invalid procedure numbers and cannot be completed.

---

### **[-badlen <Counter with Delta>] - Bad Length Calls**

Use this parameter to display information only about the RPC calls that have the number of bad length calls you specify.

### **[-badhdr <Counter with Delta>] - Bad Header Calls**

Use this parameter to display information only about the RPC calls that have the number of bad header calls you specify.

### **[-badcalls <Counter with Delta>] - Bad Calls**

Use this parameter to display information only about the RPC calls that have the number of bad calls you specify.

### **[-badprogcalls <Counter with Delta>] - Bad Program Calls**

Use this parameter to display information only about the RPC calls that have the number of bad program calls you specify.

### **[-calls <Counter64 with Delta>] - Total Calls**

Use this parameter to display information only about the RPC calls that have the total number of bad calls you specify.

## **Examples**

```
cluster1::> statistics oncrpc show-rpc-calls
```

Node	Value	Delta
node1	-----tcp-----	
Bad Proc:	0	-
Bad Len:	0	-
Bad Hdr:	0	-
Bad Calls:	0	-
Bad Prog Calls:	0	-
Total Calls:	0	-

Node	Value	Delta
node1	-----udp-----	
Bad Proc:	0	-
Bad Len:	0	-
Bad Hdr:	0	-
Bad Calls:	0	-
Bad Prog Calls:	0	-
Total Calls:	0	-

Node	Value	Delta
node2	-----tcp-----	
Bad Proc:	0	-
Bad Len:	0	-
Bad Hdr:	0	-
Bad Calls:	0	-
Bad Prog Calls:	0	-
Total Calls:	0	-

Node	Value	Delta
node2	-----udp-----	
Bad Proc:	0	-
Bad Len:	0	-
Bad Hdr:	0	-
Bad Calls:	0	-
Bad Prog Calls:	0	-
Total Calls:	0	-

---

4 entries were displayed.

---

## statistics samples delete

Delete statistics samples

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

### Description

This command deletes samples that you created using the `statistics start` command.

### Parameters

**-vserver** <vserver name> - Vserver

Selects the Vserver for which you want to delete the sample. The default Vserver is admin Vserver.

**-sample-id** <text> - Sample Identifier

Specifies the sample that you want to delete. This is a required parameter.

### Examples

The following example deletes the sample "smp1\_1":

```
cluster1::> statistics samples delete -sample-id smp1_1
```

### See Also

`statistics start`



---

## statistics samples show

Display statistics samples

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

### Description

This command displays information about the samples that you created using the `statistics start` command.

### Parameters

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

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

| [-describe ] }

Displays detailed information about each sample.

[-vserver <vserver name>] - Vserver

Selects the samples that match this parameter value. If you omit this parameter, the command displays details for all samples.

[-sample-id <text>] - Sample Identifier

Selects the samples that match this parameter value. If you do not specify this parameter, the command will display information about all the samples in the cluster.

### Examples

The following example displays information for sample "smpl\_1":

```
cluster1::> statistics samples show -sample-id smpl_1
```

Vserver	Sample ID	Start Time	Stop Time	Status
cluster-dl	smpl_1	09/13 18:06:46	-	Ready

The following example displays detailed information for sample "smpl\_1":

```
cluster1::> statistics samples show -sample-id smpl_1 -describe
```

Vserver:	vs1
Sample ID:	smpl_1
Object:	processor
Instance:	-
Counter:	-
Start Time:	09/13 18:06:46

---

```
Stop Time: -  
Status: Ready    - -  
Privilege: admin
```

## See Also

`statistics start`

---

## statistics secd show

Display SecD Statistics

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

### Description

Attention:

This command is deprecated and will be removed in a future major release.

The `statistics secd show` command displays information about SecD RPC usage statistics on the nodes in a cluster. You can view the following information:

- Number of times an RPC was called
- Number of successful RPC calls
- Number of failed RPC calls
- Maximum time taken to process an RPC
- Minimum time taken to process an RPC
- Total collective time spent on an RPC

Use this command only as directed by support personnel to help analyze performance and diagnose problems.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the nodes that match this parameter value.

---

**[-vserver <vserver>]** - Vserver

Selects the nodes that match this parameter value.

**[-secdstat-type <secdStatType>]** - SecdStatType

Selects the nodes that match this parameter value (SecD RPC type).

**[-count <Counter>]** - Count

Selects the nodes that match this parameter value (number of times an RPC was called).

**[-succeeded <Counter>]** - Success

Selects the nodes that match this parameter value (number of times an RPC succeeded).

**[-failed <Counter>]** - Failure

Selects the nodes that match this parameter value (number of times an RPC failed).

**[-total-time <Counter>]** - TotalTime

Selects the nodes that match this parameter value (total time for an RPC).

**[-max-time <Counter>]** - MaxTime

Selects the nodes that match this parameter value (maximum time for an RPC).

**[-min-time <Counter>]** - MinTime

Selects the nodes that match this parameter value (minimum time for an RPC).

## Examples

The following example displays SecD RPC call statistics for a node named node1:

```
cluster1::*> statistics secd show -node node1
```

Node:	node1					
Vserver:	vs1					
SecdStatType	Count	Success	Failure	TotalTime	MaxTime	MinTime
auth_extended	0	0	0	0	0	0
auth_passthrough	10	8	2	371240	279338	716
ontap_admin_cifs_auth_extended	0	0	0	0	0	0
ontap_admin_cifs_auth_basic	0	0	0	0	0	0
auth_get_creds	0	0	0	0	0	0
auth_user_name_to_ontap_admin_unix_creds	0	0	0	0	0	0
auth_user_name_to_unix_creds	0	0	0	0	0	0
auth_user_id_to_unix_creds	0	0	0	0	0	0
auth_user_name_to_unix_ids	0	0	0	0	0	0
auth_user_id_to_unix_owner_names	0	0	0	0	0	0
auth_user_name_to_id	0	0	0	0	0	0
auth_user_id_to_name	0	0	0	0	0	0

---

group_name_to_id	0	0	0	0	0	0
group_id_to_name	7	7	0	2857	616	318
auth_sid_to_name	0	0	0	0	0	0
auth_name_to_sid	7	7	0	2864	783	283
auth_sid_to_uid	0	0	0	0	0	0
auth_sid_to_uid_with_uid	0	0	0	0	0	0
auth_uid_to_sid	0	0	0	0	0	0
auth_uid_to_sid_with_uid	0	0	0	0	0	0
create_cifs_server	0	0	0	0	0	0
ds_change_password	0	0	0	0	0	0
ds_reset_password	3	3	0	515480	427772	29334
ds_ad_account_delete	0	0	0	0	0	0
dce_rpc_passthrough	0	0	0	0	0	0
nmap_map_name	0	0	0	0	0	0
discover_servers	0	0	0	0	0	0
discover_service	0	0	0	0	0	0
server_information	0	0	0	0	0	0
get_cifs_setup_server	0	0	0	0	0	0
nfs_krb_bind_spn	3	3	0	1306	461	398
nfs_krb_change_key	2	2	0	500443	429675	70768
nfs_krb_set_key	0	0	0	0	0	0
nfs_krb_get_key	0	0	0	0	0	0
netgroup_get_addrs	0	0	0	0	0	0
flush_netgroup_cache	0	0	0	0	0	0
accept_gss_token	0	0	0	0	0	0
handoff_gss_token	0	0	0	0	0	0
gpo_get_list	0	0	0	0	0	0

39 entries were displayed.

---

## statistics settings modify

Modify settings for the statistics commands

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

### Description

This command modifies the settings for all of the `statistics` commands.

### Parameters

**[-display-rates {true|false}]** - Display Rates

Specifies whether the `statistics` commands display rate counters in rates/second. The default is true.

### Examples

The following example sets the value of the `-display-rates` parameter to false:

```
cluster1::> statistics settings modify -display-rates false
```

### See Also

`statistics`

---

## statistics settings show

Display settings for the statistics commands

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

### Description

This command displays the current settings for all of the `statistics` commands.

### Parameters

None

### Examples

The following example displays the current settings for all `statistics` commands:

```
cluster1::> statistics settings show
Display rate Counters in rate/sec: true
```

### See Also

`statistics`

---

## statistics striping show-summary

Show sum of striped volume statistics from all nodes

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

### Description

Attention:

This command is deprecated and will be removed in a future major release.

The `statistics striping show-summary` command displays information about the striping subsystem of the cluster. The output is a series of tables which display information about different components of the striped subsystem.

The default view of the output includes three tables. The first table lists individual statistics for different data structures inside the striping subsystem. Some of the key fields displayed in this table are:

- The amount of memory used by each data structure
- The number of each type of data structure currently in use
- The number of times the system was unable to grab the data structure required due to lack of memory

The second table is a list of the individual file operations which have been served on behalf of client requests. The third table is a list of internal cross member volume operations, including the count performed, as well as a count indicating how many have failed and succeeded on both the client and the server.

The verbose view adds to the default view some extra statistics to the data regarding cross volume member operations, most notably averages for time to completion. There are two additional tables added to the output as well. The first table is a list of heartbeats and information regarding their internal state. The second new table is a summary of the CSM (Cluster Session Manager) state used for managing striped volumes.

To view information on a per-node basis for greater granularity, use the `statistics striping show` command.

### Parameters



---

## **[-verbose [true]] - Report Additional Details**

If you use this parameter the verbose view will be displayed. If you do not use this parameter, the normal output will be displayed. Passing in a value of true is supported, but not required.

## **[-diff {true|false}] - Show Change From Last Sample**

If this option is specified and set as true, only those table rows which have changed since the `statistics striping show-summary` command was last run will be displayed. Furthermore, the values displayed will not be the current value, but the change since the command was last run. This is useful for tracking which values are changing frequently when attempting to diagnose problems. If this parameter is set as false, the values returned will be the total count typically returned, as although this option had not been specified. If you enter this parameter without a value, it is set to true.

## **Examples**

The following command displays `statistics striping show-summary` output on a minimally-loaded cluster.

```
cluster1::*> statistics striping show-summary
Striping statistics for cluster:summary
```

Factory	Memory	Peak	Used	Free	Recycles	LruDry	Alloc	NoMem
DS Filetable	2457600	1	0	4096	0	0	0	0
FAS Filetable	2064384	1	0	4096	0	0	0	0
MDS Filetable	1015808	2	0	4096	0	0	0	0
Acro Filetable	6150000	0	0	9375	0	0	0	0
Striping Table	2448	1	0	1	0	0	0	0
VLDB Cache	38160	1	0	15	0	0	0	0
Volume Table	95080	3	1	4	4	1	5	0
CSM Server Call	20489728	0	0	448	65198	0	266	0
MDPE Factory	13701744	0	0	394	62071	0	250	0
Opstate	11108800	0	0	424	91341	0	0	0
Opstate CB	2515200	0	0	96	0	0	0	0
Striped Message	1592544	0	0	318	151688	0	0	0
AdminMdvState	5400	1	1	0	0	1	1	0
AdminVolState	40640	5	5	0	0	1	5	0
ResponseInfo	574400	2	0	100	63761	0	0	0
SessionInfo	16480000	5	0	20000	63758	0	0	0
Memory Blob	3581760	1	0	91	245	0	90	0
WAFL Message	120160	1	0	4	254	0	0	0
Replay Bin	7168	0	0	64	0	0	0	0
=> Total Memory	82041024							
Request	Received	Success	Failure	AvgTime	MaxTime			
Access	346	346	0	0	9			

---

Create	256	256	0	0	17
Getattr	1835	1835	0	0	177
Get_Root_FH	8	8	0	0	4
Lookup	935	556	379	0	14
Read	2886	2886	0	15	777
Readdir	3	3	0	0	0
Rename	122	122	0	4	215
Setattr	244	244	0	19	381
Unlink	191	191	0	7	48
Write	84510	83424	1086	2	890

Operation	Client-Sent	C-Success	C-Fail	S-Received	S-Success	S-Fail
DF Get Mdata	61471	61471	0	61471	61471	0
FD Inv Mdata	426	426	0	426	426	0
FM Get Mdata	600	600	0	600	600	0
MD Heartbeat	1435	1435	0	1435	1435	0
MD Perform CP	5	5	0	5	5	0
MD Perform Snap	5	5	0	5	5	0
MD Prepare Snap	5	5	0	5	5	0
MF Delete File	191	191	0	191	191	0
MF Inv Mdata	557	557	0	557	557	0
MF Set Mdata	244	244	0	244	244	0
DM Lmgr ReqLock	254	254	0	254	254	0
MD Finish Snap2	5	5	0	5	5	0

## See Also

statistics striping show

---

## statistics striping show

Show striped volume statistics

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

### Description

Attention:

This command is deprecated and will be removed in a future major release.

The `statistics striping show` command displays diagnostic information about the health and status of the striped volume system for each node specified. The output is a series of tables that display information about the striped subsystem.

The default view of the output includes three tables. The first table lists individual statistics for different data structures inside the striping subsystem. The displayed fields include:

- The amount of memory used by each data structure
- The number of each type of data structure currently in use
- The number of times the system was unable to grab the data structure required due to lack of memory

The second table is a list of the individual file operations that have been served on behalf of client requests.

The third table is a list of internal cross member volume operations, including the count performed, as well as a count of how many failed and how many succeeded on both the client and the server.

The verbose view adds statistics for cross volume member operations, most notably averages for time to completion. Also, two new tables are added to the output.

The first new table is a list of heartbeats and their internal state.

The second new table is a summary of the CSM (Cluster Session Manager) state that is used for managing striped volumes.

To display information about the whole cluster, use `statistics striping show-summary`

---

## Parameters

**-node** {<nodename>|local} - Node

Selects the nodes to report in the display.

**[-verbose [true]]** - Report Additional Details

Selects the verbose display mode. If you omit this parameter, the standard output is displayed. A value of true is supported, but not required.

**[-diff {true|false}]** - Show Change From Last Sample

If this parameter is true, only those table rows which have changed since the `statistics striping show` command was last run will be displayed. The values are not the current value, but rather the change since the command was last run. This is useful for diagnostic tracking to determine which values are changing frequently. If this parameter is false, the total counts are displayed.

## Examples

The example below displays `statistics striping show` output on a minimally-loaded system against node 'node'.

```
cluster1::*> statistics striping show -node node
Striping statistics for node
```

Factory	Memory	Peak	Used	Free	Recycles	LruDry	Alloc	NoMem
DS Filetable	2457600	1	0	4096	0	0	0	0
FAS Filetable	2064384	1	0	4096	0	0	0	0
MDS Filetable	1015808	2	0	4096	0	0	0	0
Acro Filetable	6150000	0	0	9375	0	0	0	0
Striping Table	2448	1	0	1	0	0	0	0
VLDB Cache	38160	1	0	15	0	0	0	0
Volume Table	95080	3	1	4	4	1	5	0
CSM Server Call	20489728	0	0	448	64623	0	266	0
MDPE Factory	13701744	0	0	394	62071	0	250	0
Opstate	11108800	0	0	424	91338	0	0	0
Opstate CB	2515200	0	0	96	0	0	0	0
Striped Message	1592544	0	0	318	151688	0	0	0
AdminMdvState	5400	1	1	0	0	1	1	0
AdminVolState	40640	5	5	0	0	1	5	0
ResponseInfo	574400	2	0	100	63761	0	0	0
SessionInfo	16480000	5	0	20000	63758	0	0	0
Memory Blob	3581760	1	0	91	245	0	90	0
WAFL Message	120160	1	0	4	254	0	0	0
Replay Bin	7168	0	0	64	0	0	0	0
=> Total Memory	82041024							

Request	Received	Success	Failure	AvgTime	MaxTime
Access	346	346	0	0	9
Create	256	256	0	0	17
Getattr	1835	1835	0	0	177
Get Root FH	5	5	0	0	4
Lookup	935	556	379	0	14
Read	2886	2886	0	15	777
Readdir	3	3	0	0	0
Rename	122	122	0	4	215
Setattr	244	244	0	19	381
Unlink	191	191	0	7	48
Write	84510	83424	1086	2	890

  

Operation	Client-Sent	C-Success	C-Fail	S-Received	S-Success	S-Fail
-----------	-------------	-----------	--------	------------	-----------	--------

---

DF Get Mdata	61471	61471	0	61471	61471	0
FD Inv Mdata	426	426	0	426	426	0
FM Get Mdata	600	600	0	600	600	0
MD Heartbeat	860	860	0	860	860	0
MD Perform CP	5	5	0	5	5	0
MD Perform Snap	5	5	0	5	5	0
MD Prepare Snap	5	5	0	5	5	0
MF Delete File	191	191	0	191	191	0
MF Inv Mdata	557	557	0	557	557	0
MF Set Mdata	244	244	0	244	244	0
DM Lmgr ReqLock	254	254	0	254	254	0
MD Finish Snap2	5	5	0	5	5	0

## See Also

statistics striping show-summary

---

## storage aggregate add-disks

Add disks to an aggregate

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

### Description

The `storage aggregate add-disks` command adds disks to an existing aggregate. You must specify the number of disks or provide a list of disks to be added. If you specify the number of disks without providing a list of disks, the system selects the disks.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the aggregate to which disks are to be added.

{ **[-diskcount** <integer>] - Disk Count

This parameter specifies the number of disks that are to be added to the aggregate.

**[-disktype | -T** {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SATA | SSD}] - Disk Type

This parameter specifies the type of disk that is to be added. It must be specified with the `-diskcount` parameter when adding disks to a Flash Pool.

This option is required when adding SSDs to an aggregate to convert it to a Flash Pool.

Note:

Only the aggregates marked as `hybrid_enabled` can be converted to Flash Pools. Use `storage aggregate modify` to mark the aggregate as `hybrid_enabled`.

**[-chksumstyle** <checksum style>] - Checksum Style

This parameter specifies the checksum style for the disks to be added to an aggregate. It is not applicable if `-disklist` is specified. The possible values are `block` for block checksum, `zoned` for zoned checksum and `advanced_zoned` for advanced zoned checksum (AZCS). By default, disks with the same checksum style as the aggregate are selected. This behavior can be overridden by using this parameter to create a mixed

---

checksum aggregate. A mixed checksum aggregate can support only the block and `advanced_zoned` checksum styles.

**[-simulate | -n [true]]** - Simulate addition of disks to the existing aggregate

This parameter is used with the `disktype` and `diskcount` parameters to determine which disks would be added without actually performing the addition of disks operation.

**| [-disklist | -d <disk path name>, ...]** - Disks

This parameter specifies a list of disks to be added. If you specify the `-disklist` parameter, you cannot further qualify the list of disks to be added by count, checksum style or type.

**[-allow-same-carrier [true]] }** - Allow Same RAID Group Within Carrier

This parameter can be used to allow two disks housed in the same carrier to be in the same RAID group when you add disks to an aggregate.

Having disks in the same carrier in the same RAID group is not desirable because a carrier failure can cause a simultaneous outage for two disks in the same RAID group. You can add a disk to an aggregate that causes this situation, but when an alternate disk becomes available, Data ONTAP automatically initiates a series of disk copy operations to put the disks into different RAID groups. For this reason, you should use this parameter only when necessary. When possible, allow Data ONTAP to choose disks that need to be added to the aggregate.

This parameter affects only the add-disks operation. It is not a persistent attribute of the aggregate.

**[-raidgroup | -g {new|all|<raidgroup>}]** - RAID Group

This parameter enables the administrator to specify which RAID group will receive the added disks. If this parameter is not used, the disks are added to the most recently created RAID group until it is full, then new raid groups are created and filled until all the disks are added. If a RAID group name `rgX` is specified, the disks are added to that RAID group. If `new` is specified, the disks are added to a new RAID group, even if the disks would fit into an existing RAID group. If `all` is specified, the disks are added to existing RAID groups until all existing RAID groups are full. Then Data ONTAP creates one or more new RAID groups and adds the remaining disks to the new groups. If the disk type or checksum style parameters are specified with this parameter, the command operates only on the RAID groups with the matching disk type or checksum style, even if `all` is specified.

**[-raidtype | -t {raid\_dp|raid4}]** - RAID Type

This parameter specifies the type for the new RAID groups that would be created while adding disks to the aggregate. Use this parameter when you add the first RAID group comprised of SSDs to a hybrid-enabled aggregate. The values are `raid4` for RAID 4

---

and `raid_dp` for RAID Double Parity. The default value is the type of RAID groups of the aggregate.

**[-allow-mixed-rpm | -f [true]]** - Allow Disks With Different RPM Values

This parameter specifies whether disks that have different RPM values can be added. For example, SAS disks can rotate at 10,000 or 15,000 RPM. If this parameter is set to true and a list of disks are provided by using the `-disklist` parameter, the disks will be added even if the SAS disks you specify have different RPM values. This parameter works similarly for ATA disks, which can rotate at 5,400 or 7,200 RPM.

Note:

This parameter is applicable only when the `-disklist` or `-mirror-disklist` parameter is used.

**[-64bit-upgrade <64-bit upgrade mode>]** - Mode for Upgrade to 64-bit

This parameter specifies the mode for upgrading the aggregate to 64-bit. The values are `check`, `normal`, `grow-reserved` and `grow-all`.

If `check` is specified, it displays a summary of the space impact which would result from upgrading the aggregate to 64-bit. This summary includes the space usage of each contained volume after the volume is upgraded to 64-bit and the amount of space that must be added to the volume in order to successfully complete the 64-bit upgrade. This option does not result in an upgrade to 64-bit or addition of disks.

If `normal` is specified, it upgrades the aggregate to 64-bit if the total aggregate size after adding the specified disks exceeds 16 TB. If this option is specified, the volumes will not automatically grow if they run out of space due to the 64-bit upgrade.

If `grow-reserved` is specified, it upgrades the aggregate to 64-bit if the total aggregate size after adding the specified disks exceeds 16 TB. If this option is specified, the volumes will automatically grow if they run out of space due to the 64-bit upgrade, but only to accommodate the space-reserved files within these volumes.

If `grow-all` is specified, it upgrades the aggregate to 64-bit if the total aggregate size after adding the specified disks exceeds 16 TB. If this option is specified, the volumes will automatically grow as needed if they run out of space due to the 64-bit upgrade. The volumes will grow to accommodate all the files within these volumes.

## Examples

The following example adds 10 unassigned disks to an aggregate named `aggr0`. The disks are assigned to a RAID group named `rg1`:

```
cluster1::> storage aggregate add-disks -aggregate aggr0 -diskcount 1 -raidgroup
rg1
```



---

## See Also

storage aggregate modify

---

## storage aggregate create

Create an aggregate

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

### Description

The `storage aggregate create` command creates an aggregate. An aggregate consists of disks. You must specify the number of disks or provide a list of disks to be added to the new aggregate. If you specify the number of disks without providing a list of disks, the system selects the disks.

When creating an aggregate, you can optionally specify the aggregate's home node, the RAID type for RAID groups on the aggregate, and the maximum number of disks that can be included in a RAID group.

When creating an Infinite Volume, the following types of aggregates are not supported: 32-bit and striped.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the name of the aggregate that is to be created.

{ **[-checksumstyle** <checksum style>] - Checksum Style

This parameter specifies the checksum style for the aggregate. The values are `block` for Block Checksum and `advanced_zoned` for Advanced Zoned Checksum (AZCS).

**-diskcount** <integer> - Number Of Disks

This parameter specifies the number of disks that are to be included in the aggregate, including the parity disks. The disks in this newly created aggregate come from the pool of spare disks. The smallest disks in this pool are added to the aggregate first, unless you specify the `-disksize` parameter.

**[-diskrpm | -R** <integer>] - Disk RPM

This parameter specifies the RPM of the disks on which the aggregate is to be created. Possible values include 5400, 7200, 10000, and 15000.

**[-disksize** <integer>] - Disk Size(GB)

---

This parameter specifies the size, in GB, of the disks on which the aggregate is to be created. Disks that are within 20% (plus or minus) of the specified size will be selected.

**[-disktype | -T {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SATA | SSD}]** - Disk Type

This parameter specifies the type of disk on which the aggregate is to be created.

**[-nodes {<nodename>|local}, ...]** - Nodes

This parameter specifies the home node for the aggregate. If this parameter is not specified, the node on which the command is run is set as the home node. If storage failover is configured and the home node fails, its failover partner becomes the home node.

**| -disklist | -d <disk path name>, ...** - Disks

This parameter specifies a list of disks to be added to the new aggregate. If you specify the `-disklist` parameter, you cannot further qualify the list of disks to be added by count, checksum style, type, size, or RPM.

**[-allow-same-carrier [true]] }** - Allow Same RAID Group Within Carrier

This parameter can be used to allow two disks housed in the same carrier to be in the same RAID group when you add disks to an aggregate.

Having disks in the same carrier in the same RAID group is not desirable because a carrier failure can cause a simultaneous outage for two disks in the same RAID group. You create an aggregate with this characteristic, but when an alternate disk becomes available, Data ONTAP automatically initiates a series of disk copy operations to put the disks into different RAID groups. For this reason, you should use this parameter only when necessary. When possible, allow Data ONTAP to choose the disks from which to create the aggregate.

This parameter affects only the aggregate creation operation. It is not a persistent attribute of the aggregate.

**[-allow-mixed-rpm | -f [true]]** - Allow Disks With Different RPM Values

This parameter specifies whether the aggregate can contain disks that have different RPM values. For example, SAS disks can rotate at 10,000 or 15,000 RPM. If this parameter is set to true and a list of disks are provided by using the `-disklist` parameter, the aggregate will be created even if the SAS disks you specify have different RPM values. This parameter works similarly for ATA disks, which can rotate at 5,400 or 7,200 RPM.

**[-block-type | -B {32-bit|64-bit}]** - Block Type (privilege: advanced)

---

This parameter specifies the indirect block format that the aggregate can have. The values are 32-bit and 64-bit. If you specify 64-bit, then you can create aggregates that can be larger than 16TB. The default value is 64-bit.

**[-maxraidsize | -s <integer>]** - Max RAID Size

This parameter specifies the maximum number of disks that can be included in a RAID group.

**[-raidtype | -t {raid\_dp|raid4}]** - RAID Type

This parameter specifies the type for RAID groups on the aggregate. The values are raid4 for RAID 4 and raid\_dp for RAID Double Parity. The default setting is raid\_dp . This parameter is not needed for array LUNs because they are always created with the RAID0 raidtype.

**[-simulate [true]]** - Simulate Aggregate creation

This option simulates the aggregate creation and prints the list of disks that would be used for the aggregate.

**[-skip-32bit-warning [true]]** - Skip Warning When Creating 32-bit Format Aggregate (privilege: advanced)

This parameter suppresses the confirmation when creating a 32-bit format aggregate.

**[-volume-style <flex>]** - Volume Style

This parameter specifies the volume style of the aggregate. The only supported volume style is flex. This parameter is deprecated and will be removed in a future version of Data ONTAP.

**[-force-small-aggregate [true]]** - Force the Creation of a Small Aggregate (privilege: advanced)

This parameter can be used to force the creation of a 2-disk RAID4 aggregate, or a 3-disk or 4-disk RAID-DP aggregate.

## Examples

The following example creates an aggregate named aggr0 on a home node named node0. The aggregate contains 20 disks and uses RAID-DP. The aggregate contains regular FlexVol volumes:

```
cluster1::> storage aggregate create -aggregate aggr0 -nodes node0  
-diskcount 20 -raidtype raid_dp -volume-style flex
```

The following example creates an aggregate named aggr0 on a home node named node0. The aggregate contains the disks specified and uses RAID-DP

```
cluster1::> storage aggregate create -aggregate aggr0 -nodes node0
```

---

```
-disklist 0a.15,0a.16,0a.17,0a.18,0a.19 -raidtype raid_dp
```

The following example creates an aggregate named `aggr0` on a home node named `node0`. The aggregate contains 20 disks of size 10GB and of type SAS:

```
cluster1::> storage aggregate create -aggregate aggr0 -nodes node0  
-diskcount 20 -disksize 10 -disktype SAS
```

## storage aggregate delete

Delete an aggregate

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

### Description

The `storage aggregate delete` command deletes a storage aggregate. No volumes can exist on an aggregate that is to be deleted; the command fails if volumes are present on the aggregate. The command prompts you for confirmation before running. You can use the `set` command with the `-confirmations off` parameter to disable confirmation messages.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the aggregate that is to be deleted.

**[-preserve-config-data [true]]** - Delete Physical Aggregate but Preserve Configuration Data (privilege: advanced)

Deletes the physical aggregate, but preserves the aggregate configuration data. The aggregate must not have any disks associated with it. If the parameter `-preserve-config-data` is specified without a value, the default value is `true`; if this parameter is not specified, the default value is `false`.

### Examples

The following example deletes an aggregate named `aggr1`:

```
cluster1::> storage aggregate delete -aggregate aggr1
```

### See Also

`set`

---

## storage aggregate modify

Modify aggregate attributes

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

### Description

The `storage aggregate modify` command can be used to modify an aggregate's state, RAID type, or maximum RAID group size.

Changing the RAID type immediately changes the RAID group type for all RAID groups on the aggregate. If you change the RAID type from RAID4 to RAID-DP, each RAID group allocates a spare disk for the group's second parity disk and begins a reconstruction process.

Changing the maximum RAID size does not cause existing RAID groups to grow or to shrink; rather, it affects the size of RAID groups created in the future, and determines whether more disks can be added to the RAID group that was most recently created.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the storage aggregate that is to be modified.

**[-disktype | -T {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SATA | SSD}]** - Disk Type

This parameter specifies either the HDD tier or the SSD tier when changing the RAID type of a Flash Pool. If the HDD tier is composed of more than one type of disk, specifying any of the disk types in use causes that tier to be modified.

**[-free-space-realloc {on|off|no\_redirect}]** - Free Space Reallocation

This parameter specifies whether free space reallocation is enabled on the aggregate.

Free space reallocation optimizes the free space in an aggregate immediately before Data ONTAP writes data to the blocks in that aggregate.

The default setting is `off`.

`no_redirect` is available at the diagnostic privilege level. Use the `no_redirect` option only under the guidance of support personnel.

**[-ha-policy {sfo|cfo}]** - HA Policy

---

This parameter specifies the high-availability policy to be used in the context of a root recovery procedure. Do not modify this setting unless directed to do so by a customer support representative.

**[-percent-snapshot-space <percent>]** - Space Reserved for Snapshot Copies

This parameter is used to set the space reserved for Snapshot copies to the specified value. For example, to set the snapshot reserve to 5%, you should enter `-percent-snapshot-space 5`.

**[-hybrid-enabled {true|false}]** - Hybrid Enabled

If the hybrid-enabled option is set to "true", the aggregate is marked as `hybrid_enabled`, that is, the aggregate can contain a mix of SSDs and HDDs (Hard Disk Drives, e.g., SAS, SATA, and/or FC). By default, aggregates cannot be marked "hybrid\_enabled" if the aggregate contains FlexVols that cannot be write cached. A FlexVol cannot be write-cached if it is part of an aggregate created in Data ONTAP 7. Use `-force-hybrid-enabled` to over-ride this behavior.

**[-force-hybrid-enabled | -f [true]]** - Force Marking of Aggregate as Hybrid Enabled

By default, aggregates cannot be marked "hybrid\_enabled" if the aggregate contains FlexVols that cannot be write cached. A FlexVol cannot be write-cached if it is part of an aggregate created in Data ONTAP 7. Use `-force-hybrid-enabled` to over-ride this behavior. Note that read caching will be enabled on these FlexVols, but write caching will be disabled. Setting this parameter to true would mark the aggregate as `hybrid_enabled`; this means that the aggregate can contain a mix of SSDs and HDDs (Hard Disk Drives, for example, SAS, SATA and/or FC). This parameter is used to force marking aggregates which have FlexVols that cannot be write cached as hybrid enabled. FlexVols in the aggregate marked as hybrid enabled using this parameter which cannot participate in write-caching will only have read-caching enabled. All other FlexVols in the aggregate can participate in both read and write caching.

**[-maxraidspace | -s <integer>]** - Max RAID Size

This parameter specifies the maximum number of disks that can be included in a RAID group for this aggregate.

Note:

For Flash Pools, this option controls the maximum size of the HDD RAID groups.

**[-cache-raid-group-size <integer>]** - Flash Pool SSD Tier Maximum RAID Group Size

This parameter specifies the maximum number of disks that can be included in a SSD RAID group for this Flash Pool.

Note:

---

This parameter is applicable only for Flash Pools.

**[-raidtype | -t {raid\_dp|raid4}]** - RAID Type

This parameter specifies the RAID type for RAID groups on the aggregate. Possible values are `raid4` for RAID 4 and `raid_dp` for RAID-DP.

**[-state <aggregate state>]** - State

This deprecated parameter specifies the state of the aggregate. Possible values are as follows:

- **online** - Immediately sets the aggregate online. All volumes on the aggregate are set to the state they were in when the aggregate was taken offline or restricted. The preferred command to bring an aggregate online is `storage aggregate online`.
- **offline** - Takes an aggregate offline. You cannot take an aggregate offline if any of its volumes are online. The preferred command to take an aggregate offline is `storage aggregate offline`.
- **restricted** - Restricts the aggregate. You cannot restrict an aggregate if any of its volumes are online. The preferred command to restrict an aggregate is `storage aggregate restrict`.

## Examples

The following example changes all RAID groups on an aggregate named `aggr0` to use RAID-DP.

```
cluster1::> storage aggregate modify -aggregate aggr0 -raidtype raid_dp
```

## See Also

`storage aggregate scrub`   `storage aggregate online`   `storage aggregate offline`  
`storage aggregate restrict`



---

## storage aggregate offline

Offline an aggregate

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

### Description

The `storage aggregate offline` command takes an aggregate offline.

If you are taking a root aggregate offline, the node owning the aggregate must be in maintenance mode.

### Parameters

**-aggregate** <aggregate name> - Aggregate

The name of the aggregate to be taken offline.

### Examples

The following example takes an aggregate named `aggr1` offline:

```
cluster1::> storage aggregate offline -aggregate aggr1
```

### See Also

[storage aggregate online](#)

---

## storage aggregate online

Online an aggregate

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

### Description

The `storage aggregate online` command brings an aggregate online if the aggregate is in offline or restricted state. If an aggregate is in an inconsistent state, it must be brought to a consistent state before it can be brought online. If you have an aggregate that is in an inconsistent state, contact technical support.

### Parameters

**-aggregate** <aggregate name> - Aggregate

The name of the aggregate to be brought online.

### Examples

The following example brings an aggregate named `aggr1` online:

```
cluster1::> storage aggregate online -aggregate aggr1
```

### See Also

`storage aggregate offline`   `storage aggregate restrict`

---

## storage aggregate rename

Rename an aggregate

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

### Description

The `storage aggregate rename` command renames an aggregate.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the aggregate to be renamed.

**-newname** <aggregate name> - New Name

This parameter specifies the new name for the aggregate.

### Examples

The following example renames an aggregate named `aggr5` as `sales-aggr`:

```
cluster1::> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

## storage aggregate restrict

Restrict an aggregate

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

### Description

The `storage aggregate restrict` command puts an aggregate in restricted state to make data in the aggregate's volumes unavailable to clients. When an aggregate is in restricted state data access is not allowed. However, few operations such as aggregate copy, parity recomputation, scrub and RAID reconstruction are allowed. You can also use this command if you want the aggregate to be the target of an aggregate copy or SnapMirror replication operation.

---

## Parameters

**-aggregate** <aggregate name> - Aggregate

The name of the aggregate to be restricted.

## Examples

The following example restricts an aggregate named aggr1:

```
cluster1::> storage aggregate restrict -aggregate aggr1
```

## See Also

storage aggregate show

---

## storage aggregate scrub

Aggregate parity scrubbing

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

### Description

The `storage aggregate scrub` command scrubs an aggregate for media and parity errors. Parity scrubbing compares the data disks to the parity disks in their RAID group and corrects the parity disks contents, as required. If no name is given, parity scrubbing is started on all online aggregates.

Note:

By default, scrubs are scheduled to run for a specified time on a weekly basis. However, you can use this command to run scrubs manually to check for errors and data inconsistencies.

### Parameters

**-aggregate** <aggregate name> - Aggregate

This parameter specifies the aggregate to be scrubbed for errors.

**[-raidgroup <text>]** - RAID Group

This parameter specifies the RAID group to be scrubbed. If this parameter is not specified, the command scrubs the entire aggregate.

**-action** {start|stop|resume|suspend|status} - Action

This parameter specifies the action to be taken. The possible actions are:

- start - Starts a scrub.
- stop - Permanently stops a scrub. A stopped scrub cannot be resumed.
- resume - Resumes a suspended parity scrub.
- suspend - Suspends a parity scrub.
- status - Displays the current status of a scrub.

### Examples

---

The following example starts a scrub on a RAID group named rg0 on an aggregate named aggr0:

```
cluster1::> storage aggregate scrub -aggregate aggr0 -raidgroup rg0 -action start
```

The following example queries the status of a scrub:

```
cluster1::> storage aggregate scrub -aggregate aggr0 -raidgroup rg0 -action  
status
```

```
Raid Group:/aggr0/plex0/rg0, Is Suspended:false, Last Scrub:Sun Nov 13  
01:30:55 2011  
, Percentage Completed:7%
```

---

## storage aggregate show-scrub-status

Display aggregate scrubbing status

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

### Description

The `storage aggregate show-scrub-status` command displays the following information about the scrub status of aggregates:

- Aggregate name
- RAID groups
- Whether the scrub is suspended
- Percentage of the scrub that is completed
- Last scrub time of the aggregate

### Parameters

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

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

| [-**instance** ] }

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

[-**aggregate** <aggregate name>] - Aggregate

If this parameter is specified, the command displays detailed scrub-status information about the specified aggregate.

[-**raidgroup** <text>] - RAID Group

If this parameter is specified, the command displays information only about the aggregate that contains the specified RAID group.

[-**suspended** {true|false}] - Is Suspended

---

If this parameter is specified, the command displays information only about the aggregates that have the specified scrub-suspension state (true or false).

**[-complete-percentage <percent>]** - Percentage Completed

If this parameter is specified, the command displays information only about the aggregates whose scrubs have the specified completed percentage.

**[-last-scrub-time <MM/DD/YYYY HH:MM:SS>]** - Last Scrub Time

If this parameter is specified, the command displays information only about the aggregates that have the specified last-scrub time, in the format MM/DD/YYYY HH:MM:SS.

## Examples

The following example displays scrub-status information for all the aggregates:

```
cluster1::> storage aggregate show-scrub-status
Aggregate RAID Groups      Suspended  Percentage Last Scrub Time
-----
aggr0      /aggr0/plex0/rg0      true        0% 3/31/2011  21:23:02
aggr1      /aggr1/plex0/rg1      true        45% 3/30/2011  01:05:00
aggr2      /aggr2/plex0/rg0      true        33% 3/30/2011  23:43:34
aggr3      /aggr3/plex0/rg1      true        79% 3/29/2011  00:34:36
4 entries were displayed.
```

The following example displays detailed information about the aggregate named aggr1:

```
cluster1::> storage aggregate show-scrub-status -instance -aggregate aggr1
Aggregate: aggr1
RAID Group: /aggr1/plex0/rg0
Is Suspended: false
Percentage Completed: 2%
Last Scrub Time: 3/31/2011 22:02:50
```

## See Also

storage aggregate scrub



---

## storage aggregate show-space

Display details of space utilization within an aggregate.

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

### Description

The `storage aggregate show-space` command displays information about space utilization within aggregates. The command output breaks down space usage in the specified aggregate by feature. If no parameters are specified, the command displays this information about all aggregates:

### Parameters

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

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

| [-instance ] }

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

[-aggregate <aggregate name>] - Aggregate

If this parameter is specified, the command displays information only about space used in the specified aggregate or aggregates.

[-volume-footprints {<integer>[KB|MB|GB|TB|PB]] - Volume Footprints

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified amount of space in use by volume footprints. A volume's footprint is the overall amount of space that a volume occupies in the aggregate, including the volume metadata and data.

[-volume-footprints-percent <percent>] - Volume Footprints Percent

If this parameter is specified, the command displays information only about the aggregate or aggregates whose volume footprints occupy the specified percentage of space.

**[-snap-size-total {<integer>[KB|MB|GB|TB|PB]]** - Total Space for Snapshot Copies in Bytes

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified amount of space in use by aggregate Snapshot copies. This field includes the space that is reserved for Snapshot copies and is not available to volumes or aggregate data and metadata. It is set to 0 by default.

**[-percent-snapshot-space <percent>]** - Space Reserved for Snapshot Copies

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified percentage of space in use by aggregate Snapshot copies.

**[-aggregate-metadata {<integer>[KB|MB|GB|TB|PB]]** - Aggregate Metadata

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified amount of space in use by aggregate metadata.

**[-aggregate-metadata-percent <percent>]** - Aggregate Metadata Percent

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified percentage of space in use by aggregate metadata.

**[-used-including-snapshot-reserve {<integer>[KB|MB|GB|TB|PB]]** - Total Used

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified amount of space in use in the aggregate.

It is important to note that this parameter treats the entire Snapshot reserve as used space since it is not available for volumes.

**[-used-including-snapshot-reserve-percent <percent>]** - Total Used Percent

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified percentage of space in use in the aggregate and its Snapshot reserve.

## Examples

The following example displays information about all aggregates:

```
cluster1::> storage aggregate show-space
Aggregate : agr0
Feature-----
Volume Footprints      856.3MB      95%
```

---

Aggregate Metadata	216KB	0%
Total Used	856.5MB	95%
Aggregate : theaggr		
Feature	Used	Used%
-----	-----	-----
Volume Footprints	2.03GB	77%
Aggregate Metadata	256KB	0%
Total Used	2.03GB	77%

2 entries were displayed.

---

## storage aggregate show

Display a list of aggregates

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

### Description

The `storage aggregate show` command displays information about aggregates. By default, the command displays the following information:

- Aggregate name
- Size
- Available size
- Percentage used
- State
- Number of volumes
- Node or nodes on which the aggregate is located
- RAID status

To display detailed information about a single aggregate, use the `-aggregate` parameter.

### Parameters

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

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

| **[-checksum ]**

Displays this information about the checksum for all aggregates:

- Aggregate name
- Checksum status (active, off, reverting, none, unknown, initializing, reinitializing, reinitialized, upgrading\_phase1, or upgrading\_phase2)

- 
- Checksum style (none, advanced\_zoned, zoned, block, mixed, WAFL, or unknown)

| **[-disk ]**

Displays disk names for all aggregates:

- Aggregate name
- Number and names of disks in the aggregate

| **[-raid-info ]**

Displays information about RAID groups, RAID type, maximum RAID size, checksum state, checksum style and whether the RAID status is inconsistent.

| **[-instance ] }**

Displays detailed information about all aggregates.

**[-aggregate <aggregate name>]** - Aggregate

If this parameter is specified, the command displays detailed information about the specified aggregate.

**[-checksumstyle <checksum style>]** - Checksum Style

Selects the aggregates that match this parameter value.

**[-diskcount <integer>]** - Number Of Disks

Selects the aggregates that match this parameter value.

**[-nodes {<nodename>|local}, ...]** - Nodes

Selects the aggregates that match this parameter value.

**[-disklist | -d <disk path name>, ...]** - Disks

Selects the aggregates that match this parameter value.

**[-free-space-realloc {on|off|no\_redirect}]** - Free Space Reallocation

Selects the aggregates that match this parameter value.

**[-ha-policy {sfo|cfo}]** - HA Policy

Selects the high-availability policy to be used in the context of a root recovery procedure. Do not modify this setting unless directed to do so by a customer support representative.

**[-percent-snapshot-space <percent>]** - Space Reserved for Snapshot Copies

---

Selects the aggregates that match this parameter value.

**[-hybrid-enabled {true|false}]** - Hybrid Enabled

Selects the aggregates that are eligible to contain both SSD and non-SSD RAID groups.

**[-availsize {<integer>[KB|MB|GB|TB|PB]}]** - Available Size

Selects the aggregates that match this parameter value.

**[-block-type | -B {32-bit|64-bit}]** - Block Type (privilege: advanced)

Selects the aggregates that match this parameter value.

**[-checksumenabled {true|false}]** - Checksum Enabled

Selects the aggregates that match this parameter value.

**[-checksumstatus <text>]** - Checksum Status

Selects the aggregates that match this parameter value. Possible values for checksum status include the following: active, off, reverting, none, unknown, initializing, reinitializing, reinitialized, upgrading\_phase1, and upgrading\_phase2.

**[-has-mroot {true|false}]** - Has Mroot Volume

Selects the aggregates that contain their owning node's management root directory.

**[-has-partner-mroot {true|false}]** - Has Partner Node Mroot Volume

Selects the aggregates that contain the management root directory of their owning node's failover partner.

**[-home-id <integer>]** - Home ID

Selects the aggregates whose home node has the specified system ID.

**[-home-name <text>]** - Home Name

Selects the aggregates whose home node is the specified node.

**[-hybrid-cache-size-total {<integer>[KB|MB|GB|TB|PB]}]** - Total Hybrid Cache Size

Selects the aggregates that have the specified total cache size in a Flash Pool.

**[-hybrid {true|false}]** - Hybrid

Selects the aggregates that currently contain both SSD and non-SSD RAID groups. Flash Pools are not supported in Data ONTAP 8.1.0.

**[-inconsistent {true|false}]** - Inconsistent

Selects the aggregates that match this parameter value.

**[-is-home {true|false}]** - Is Aggregate Home

---

Selects the aggregates whose home node and owner node have the same system ID.

**[-maxraidsize | -s <integer>]** - Max RAID Size

Selects the aggregates that match this parameter value.

Note:

For Flash Pools, this option controls the maximum size of the HDD RAID groups.

**[-cache-raid-group-size <integer>]** - Flash Pool SSD Tier Maximum RAID Group Size

Selects the aggregates that match this parameter value.

Note:

This parameter is applicable only for Flash Pools.

**[-owner-id <integer>]** - Owner ID

Selects the aggregates that match this parameter value.

**[-owner-name <text>]** - Owner Name

Selects the aggregates that match this parameter value.

**[-percent-used <percent>]** - Used Percentage

Selects the aggregates that match this parameter value.

**[-plexes <text>, ...]** - Plexes

Selects the aggregates that match this parameter value.

**[-raidgroups <text>, ...]** - RAID Groups

Selects the aggregates that match this parameter value.

**[-raidstatus <text>]** - RAID Status

Selects the aggregates that match this parameter value. Possible values for RAID status are normal, copying, ironing, degraded, growing, initializing, invalid, needs check, partial, reconstruct, raid4, raid0, raid\_dp, redirect, and waf in inconsistent. You can specify multiple values (for example, reconstruct,growing).

**[-raidtype | -t {raid\_dp|raid4}]** - RAID Type

Selects the aggregates that match this parameter value.

**[-root {true|false}]** - Is Root

Selects the aggregates that match this parameter value.

**[-sis-metadata-space-used {<integer>[KB|MB|GB|TB|PB]}]** - Space Used by Metadata for Volume Efficiency

Selects aggregates with the specified space used by A-SIS metafiles for volume efficiency. This parameter is deprecated in Data ONTAP 8.2 and later. Use the volume-footprint-list-info API for details related to space usage by deduplication metadata

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

Selects the aggregates that match this parameter value.

**[-state <aggregate state>]** - State

Selects the aggregates that match this parameter value.

**[-usedsize {<integer>[KB|MB|GB|TB|PB]}]** - Used Size

Selects the aggregates that match this parameter value.

**[-uuid <text>]** - UUID (privilege: advanced)

Selects the aggregates that match this parameter value.

**[-volcount <integer>]** - Number Of Volumes

Selects the aggregates that match this parameter value.

**[-volume-style <flex>]** - Volume Style

If this parameter is specified, the command displays information only about the aggregate or aggregates that have the specified volume style. The only supported volume style is flex. This option is deprecated and will be removed in a future version of Data ONTAP.

## Examples

The following example displays information about all aggregates:

```
cluster1::> storage aggregate show
Aggregate      Size Available Used% State  #Vols Nodes  RAID Status
-----
aggr0          6.21TB    1.78TB    71% online    49 node0  raid_dp,
normal
aggr1          56.04MB    55.89MB     0% online     0 node1  raid_dp,
normal
aggr2          1.77TB    1.63TB     8% online     1 node2  raid_dp,
normal
aggr3          1.77TB    1.73TB     2% online     2 node3  raid_dp,
normal
4 entries were displayed.
```

The following example displays information about an aggregate name aggr1:

```
cluster1::> storage aggregate show -aggregate aggr1
Aggregate: aggr1
Checksum Style: block
Number Of Disks: 3
Nodes: node1
```



---

```

Disks: node1:v3.10,
      node1:v3.20,
      node1:v3.21
Free Space Reallocation: off
                        HA Policy: sfo
Space Reserved for Snapshot Copies: -
Hybrid Enabled: false
Available Size: 55.89MB
Block Type: 64-bit
Checksum Enabled: true
Checksum Status: active
Has Mroot Volume: false
Has Partner Node Mroot Volume: false
Home ID: 4035150898
Home Name: node1
Total Hybrid Cache Size: 0B
Hybrid: false
Inconsistent: false
Is Aggregate Home: true
Max RAID Size: 16
Hybrid Aggregate SSD Tier Maximum RAID Group Size: -
Owner ID: 4035150898
Owner Name: node1
Used Percentage: 0%
Plexes: /aggr1/plex0
RAID Groups: /aggr1/plex0/rg0 (block)
RAID Status: raid_dp, normal
RAID Type: raid_dp
Is Root: false
Space Used By metadata for Volume Efficiency: 0B
Size: 56.04MB
State: online
Used Size: 152KB
Number Of Volumes: 0
Volume Style: flex

```

---

## storage aggregate 64bit-upgrade status

Display the status of 64-bit upgrade on an aggregate

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

### Description

The `storage aggregate 64bit-upgrade status` command displays the status of the 64-bit upgrade scanner of a storage aggregate and its contained flexible volumes. By default only aggregates and flexible volumes currently upgrading are listed.

### Parameters

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

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

| [-instance ] }

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

**[-aggregate <aggregate name>]** - Aggregate

This specifies the storage aggregate for which to display scanner status.

**[-vserver <text>]** - Vserver Name

If this parameter is specified, the command displays information only about the aggregate's contained volumes which are also on the specified Vserver, even if there is no upgrade in progress on those volumes.

**[-volume <text>]** - Volume Name

If this parameter is specified, the command displays information only about the aggregate's contained volumes matching the specified name, even if there is no upgrade in progress on those volumes.

**[-include-all-volumes [true]]** - Include All Volumes

If this parameter is specified, the command displays the scanner status for the aggregate and all of its contained flexible volumes, even those where no upgrade is in progress.

---

**[-format {64-bit|32-bit|upgrading}] - Format**

If this parameter is specified, the command displays information only about the aggregate or its contained flexible volumes with the specified block format, even if there is no upgrade in progress.

**[-scanner-status {running|stopped}] - Scanner Status**

If this parameter is specified, the command displays information only about the aggregate or its contained flexible volumes for which the upgrade scanner status matches the specified status, even if there is no upgrade in progress.

**[-scan-percent-completed <percent>] - Upgrade Scan Percent Completed**

If this parameter is specified, the command displays information only about the aggregate or its contained flexible volumes for which the upgrade scanner has completed the specified percentage, even if there is no upgrade in progress.

**[-scan-time-to-complete <timeticks>] - Time to Complete Scan**

If this parameter is specified, the command displays information only about the aggregate or its contained flexible volumes for which the upgrade scanner has the specified estimated time to completion, even if there is no upgrade in progress.

**[-scan-progress <text>] - Scan Progress**

If this parameter is specified, the command displays information only about the aggregate or its contained flexible volumes for which the upgrade scanner has the specified progress string, even if there is no upgrade in progress.

## Examples

The following example displays the upgrade scanner progress of only the storage aggregate or flexible volumes that are currently upgrading:

```
cluster1::*> storage aggregate 64bit-upgrade status -aggregate aggr1
Aggregate Vserver   Volume      Format      Scanner    Done  Time to  Progress
-----
aggr1      vs1              vol1        upgrading  running  98%    00:00    fbn 0, inode
                                         102 of 630,
                                         public
                                         fbn 0, inode
                                         78 of 630,
                                         private
                                         2 entries were displayed.
```

The following example displays the upgrade scanner progress of the storage aggregate and all its contained volumes:

```
cluster1::*> storage aggregate 64bit-upgrade status -aggregate aggr1 -include-
all-volumes
Aggregate Vserver   Volume      Format      Scanner    Done  Time to  Progress
-----
```

---

aggr1	-	-	64-bit	-	-	-	-	-
	vs1	vol1	upgrading	running	99%	00:00	fbn 0, inode	
							69 of 630,	
		vol2	64-bit	-	-	-	private	
		vol3	upgrading	running	76%	00:01	fbn 0, inode	
							90 of 630,	
							private	

4 entries were displayed.

---

## storage aggregate relocation show

Display relocation status of an aggregate

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

### Description

The `storage aggregate relocation show` command displays status of aggregates which were relocated in the last instance of relocation operation.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects aggregates from the specified source node.

[-**aggregate** <text>] - Aggregate Name

Selects the aggregates that match this parameter value.

[-**relocation-status** <text>] - Aggregates Relocation Status

Selects the aggregates whose relocation status matches this parameter value.

[-**destination** <text>] - Destination for Relocation

Selects the aggregates that are designated for relocation on the specified destination node.

### Examples

The following example displays the relocation status of aggregates on all nodes in the cluster:

```
cluster1::> storage aggregate relocation show
Source      Aggregate  Destination  Relocation Status
-----
node0
```

---

node1	-	-	Not attempted yet
	aggr1	node0	Done
	aggr2	node0	In progress
	aggr3	node0	Not attempted yet
4 entries were displayed.			

---

## storage aggregate relocation start

Relocate aggregates to the specified destination

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

### Description

The `storage aggregate relocation start` command initiates the relocation of the aggregates from one node to the other node in the same cluster.

### Parameters

**-node** {<nodename>|local} - Name of the Node that currently owns the aggregate

This specifies the source node where the aggregates to be relocated reside.

**-destination** {<nodename>|local} - Destination node

This specifies the destination node where aggregates are to be relocated.

**-aggregate-list** <aggregate name>, ... - List of Aggregates to be relocated

This specifies the list of aggregate names to be relocated from source node to destination node.

**[-override-vetoes]** {true|false} - Override Vetoes

This specifies whether to override the veto checks for relocation operation. Initiating aggregate relocation with vetoes overridden will result in relocation proceeding even if the node detects outstanding issues that would make aggregate relocation dangerous or disruptive. The default value is false.

**[-relocate-to-higher-version]** {true|false} - Relocate To Higher Version

This specifies if the aggregates are to be relocated to a node which is running on a higher version of Data ONTAP than the source node. If an aggregate is relocated to this destination then that aggregate cannot be relocated back to the source node till the source is also upgraded to the same or higher Data ONTAP version. This option is not required if the destination node is running on higher minor version, but the same major version. The default value is false.

**[-override-destination-checks]** {true|false} - Override Destination Checks

This specifies if the relocation operation should override the check done on destination node. This option could be used to force a relocation of aggregates even if the

---

destination has outstanding issues. Note that this could make the relocation dangerous or disruptive. The default value is false.

**[-ndo-controller-upgrade {true|false}]** - Relocate Aggregates for NDO Controller Upgrade (privilege: advanced)

This specifies if the relocation operation is being done as a part of non-disruptive controller upgrade process. Aggregate relocation will not change the home ownerships of the aggregates while relocating as part of controller upgrade. The default value is false.

## Examples

The following example relocates aggregates name aggr1 and aggr2 from source node node0 to destination node node1:

```
cluster1::> storage_aggregate relocation start -node node0 -destination node1 -
aggregate-list aggr1, aggr2
```

## storage array modify

Make changes to an array's profile.

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

## Description

The `storage array modify` command lets the user change several array parameters.

## Parameters

**-name <text>** - Name

Storage array name, either generated by Data ONTAP or assigned by the user.

**[-prefix <text>]** - Prefix

Abbreviation for the named array.

**[-vendor <text>]** - Vendor

Array manufacturer.

**[-model <text>]** - Model

Array model number.



---

**[-options <text>]** - options

Vendor specific array settings.

**[-max-queue-depth <integer>]** - Target Port Queue Depth (privilege: advanced)

The target port queue depth for all target ports on this array.

**[-lun-queue-depth <integer>]** - LUN Queue Depth (privilege: advanced)

The queue depth assigned to array LUNs from this array.

**[-is-upgrade-pending {true|false}]** - Upgrade Pending (privilege: advanced)

The is-upgrade-pending status for the array.

## Examples

This command changes the model to FastT.

```
vnv3070f20b:> storage array modify -name IBM_1722_1 -model FastT
```

## storage array remove

Remove a storage array record from the array profile database.

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

## Description

The `storage array remove` command discards array profile records for a particular storage array from the cluster database. Upon command completion, if a storage array is still connected to the cluster, the array profile record is re-created with default values.

## Parameters

**-name <text>** - Name

Name of the storage array you want to remove from the database.

## Examples

```
vnv3070f20b:> storage array remove IBM_1722_1
```

---

## storage array rename

Change the name of a storage array in the array profile database.

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

### Description

The `storage array rename` command permits substitution of the array profile name which Data ONTAP assigned during device discovery. By default, the name that Data ONTAP assigned to the storage array during discovery is shown in Data ONTAP displays and command output.

### Parameters

**-name** <text> - Name

Storage array name either generated by Data ONTAP or assigned by the user.

**-new-name** <text> - The new name to assign to this array profile. (28 chars max)

New name to assign to the storage array.

### Examples

```
vnv3070f20b::> storage array rename -name HITACHI_DF600F_1 -new-name MyArray
```

## storage array show

Display information about SAN-attached storage arrays.

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

### Description

The `storage array show` command displays information about arrays visible to the cluster. If no parameters are specified, the command displays the following information about all storage arrays:

- Prefix
- Name

- 
- Vendor
  - Model
  - Options

To display detailed information about a single array, use the `-name` parameter. The detailed view adds the following information:

- Serial Number
- Optimization Policy
- Affinity
- Errors

## Parameters

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

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

| **[-instance ]** }

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

**[-name <text>]** - Name

Selects the arrays that match this parameter value.

**[-prefix <text>]** - Prefix

Abbreviation for the named array.

**[-vendor <text>]** - Vendor

Array manufacturer.

**[-model <text>]** - Model

Array model number.

**[-options <text>]** - options

Vendor specific array settings.

**[-serial-number <text>]** - Serial Number

Array product identifier.

---

**[-max-queue-depth <integer>]** - Target Port Queue Depth (privilege: advanced)

Selects the arrays that match this parameter value.

**[-lun-queue-depth <integer>]** - LUN Queue Depth (privilege: advanced)

Selects the arrays that match this parameter value.

**[-is-upgrade-pending {true|false}]** - Upgrade Pending (privilege: advanced)

Selects the arrays that match this parameter value.

**[-optimization-policy {iALUA|eALUA|symmetric|proprietary|mixed|unknown}]** - Optimization Policy

Selects the arrays that match this parameter value.

**[-affinity {none|aaa|ap|mixed|unknown}]** - Affinity

Selects the arrays that match this parameter value.

**[-error-text <text>, ...]** - Error Text

Selects the arrays that match this parameter value.

## Examples

The following example displays information about all arrays.

```
cluster1::> storage array show
Prefix      Name      Vendor      Model Options
-----
                HITACHI_DF600F_1  HITACHI      DF600F
                IBM_1722_1      IBM          1722
2 entries were displayed.
```

The following example displays detailed information about a specific array:

```
cluster1::> storage array show -name HITACHI_DF600F_1
      Name: HITACHI_DF600F_1
      Prefix: abc
      Vendor: HITACHI
      Model: DF600F
      options:
      Serial Number: 4291000000000000
      Optimization Policy: iALUA
      Affinity: aaa
      Error Text:
```

---

## storage array config show

Display connectivity to back-end storage arrays.

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

### Description

The `storage array config show` command displays information about how the storage arrays connect to the cluster, LUN groups, number of LUNS, and more. Use this command to validate the Cluster-Mode configuration and to assist in troubleshooting.

### Parameters

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

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

| [-switch ]

If you specify this parameter, switch port information is shown.

| [-instance ] }

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

**[-node {<nodename>|local}]** - Controller Name

Selects the arrays that match this parameter value.

**[-group <integer>]** - LUN Group

Selects the arrays that match this parameter value. A LUN group is a set of LUNs that shares the same path set.

**[-target-wwpn <text>]** - Array Target Ports

Selects the arrays that match this parameter value (the World Wide Port Name of a storage array port).

**[-initiator <text>]** - Initiator

Selects the arrays that match this parameter value (the host bus adapter that the clustered node uses to connect to storage arrays).

---

**[-array-name <array name>]** - Array Name

Selects the arrays that match this parameter value.

**[-target-side-switch-port <text>]** - Target Side Switch Port

Selects the arrays that match this parameter value.

**[-initiator-side-switch-port <text>]** - Initiator Side Switch Port

Selects the arrays that match this parameter value.

**[-lun-count <integer>]** - Number of array LUNs

Selects the arrays that match this parameter value.

**[-ownership {all|assigned|unassigned}]** - Ownership

Selects the arrays that match this parameter value.

## Examples

```
cluster1::> storage array config show
```

Node Initiator	LUN Group	LUN Count	Array Name	Array Target Port
node1	0	20	DGC_RAID5_1	5006016030229f13
0d				5006016130229f13
0c				5006016830229f13
0b				5006016930229f13
0a	1	21	HITACHI_OPEN_1	50060e80034fe704
0c				50060e80034fe714
0d				50060e80034fe715
0a				50060e80034fe716
0b				50060482cb1bce1d
0b				5006048ach1bce0c
0c				202600a0b8322d10
0d	2	8	EMC_SYMMETRIX_1	204700a0b8322d10
0a				5006016030229f13
0b				5006016030229f13
0c				5006016030229f13
0d	3	10	IBM_UniversalXport_1	202600a0b8322d10
0a				204700a0b8322d10
0b				202600a0b8322d10
node2	0	20	DGC_RAID5_1	5006016030229f13
0d				5006016030229f13

---

0c				5006016130229f13
0b				5006016830229f13
0a				5006016930229f13
0c	1	21	HITACHI_OPEN_1	50060e80034fe704
0d				
0a				50060e80034fe714
0b				
0b				50060e80034fe715
0c				50060e80034fe716
0d				
0a	2	8	EMC_SYMMETRIX_1	50060482cb1bce1d
0b				
0c				5006048acb1bce0c
0d				
0c	3	10	IBM_UniversalXport_1	202600a0b8322d10
0d				
0a				204700a0b8322d10

0b  
38 entries were displayed.

Warning: Configuration errors were detected. Use 'storage errors show' for detailed information.

---

## storage array port modify

Make changes to a target port record.

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

### Description

The `storage array port modify` command lets the user change array target port parameters.

### Parameters

**-name** <text> - Name

Selects the array ports that match this parameter value. The storage array name is either generated by Data ONTAP or assigned by the user.

**-wwnn** <text> - WWNN

Selects the array ports that match this parameter value.

**-wwpn** <text> - WWPN

Selects the array ports that match this parameter value.

**[-max-queue-depth <integer>]** - Target Port Queue Depth

The target port queue depth for this target port.

### Examples

This command changes the maximum queue depth for this target port to 32.

```
vnv3070f20b::> storage array port modify -name HITACHI_DF600F_1 -wwnn  
50060e80004291c0 -wwpn 50060e80004291c0 -max-queue-depth 32
```

## storage array port remove

Remove a port record from an array profile.

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



---

## Description

The `storage array port remove` command removes a port from the array database. You might want to remove ports that are no longer connected to the clustered node. Port information can change after hardware replacement, rezoning, or similar configuration activities. The database retains the records about previous ports unless you remove the information.

## Parameters

**-name** <text> - Name

Selects the array ports that match this parameter value. The storage array name is either generated by Data ONTAP or assigned by the user.

**-wwnn** <text> - WWNN

Selects the array ports that match this parameter value.

**-wwpn** <text> - WWPN

Selects the array ports that match this parameter value.

## Examples

This command removes a port record from the array profiles database.

```
vnv3070f20b::> storage array port remove -name HITACHI_DF600F_1 -wwnn  
50060e80004291c0 -wwpn 50060e80004291c0
```

## storage array port show

Display information about a storage array's target ports.

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

## Description

The `storage array port show` command displays all the target ports known to the cluster for a given storage array (if an array name is specified) or for all storage arrays if no storage array name is specified. Target ports remain in the database as part of an array profile unless you explicitly remove them from the database.

## Parameters

---

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

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

| [-**instance** ] }

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

[-**name** <text>] - Name

Selects the array ports that match this parameter value. The storage array name is either generated by Data ONTAP or assigned by the user.

[-**wwnn** <text>] - WWNN

Selects the array ports that match this parameter value.

[-**wwpn** <text>] - WWPN

Selects the array ports that match this parameter value.

[-**max-queue-depth** <integer>] - Target Port Queue Depth

Selects the array ports that match this parameter value.

[-**node** {<nodename>|local}, ...] - Controller Name

Selects the array ports that match this parameter value.

[-**initiator-port** <text>, ...] - Initiator Port

Selects the array ports that match this parameter value.

[-**average-latency-per-iop** <integer>, ...] - Average Latency Per IOP

Selects the array ports that match this parameter value.

[-**average-pending** <integer>, ...] - Average Pending (privilege: advanced)

Selects the array ports that match this parameter value (average over time of how many commands are on the outstanding queue).

[-**average-waiting** <integer>, ...] - Average Waiting (privilege: advanced)

Selects the array ports that match this parameter value (average over time of how many commands are on the waiting queue).

[-**connection-type** {direct|fabric}] - Connection Type

Selects the array ports that match this parameter value (type of connection between the controller and the back end storage).

---

**[-max-pending <integer>, ...]** - Max Pending (privilege: advanced)

Selects the array ports that match this parameter value (largest number of commands observed on the outstanding queue).

**[-max-waiting <integer>, ...]** - Max Waiting (privilege: advanced)

Selects the array ports that match this parameter value (largest number of commands observed on the waiting queue).

**[-path-link-errors <integer>, ...]** - Link Error count on path

Selects the array ports that match this parameter value.

**[-percent-busy <integer>, ...]** - Percent Busy

Selects the array ports that match this parameter value (percentage of time I/Os are outstanding on the port).

**[-percent-waiting <integer>, ...]** - Percent Waiting

Selects the array ports that match this parameter value (percentage of time there are I/Os waiting on the throttle list on the target port).

**[-switch-port <text>]** - Switch Port

Selects the array ports that match this parameter value (for fabric attached connections, the switch port the array target port is connected to; N/A for direct attached).

**[-target-io-kbps <integer>, ...]** - Kbytes of I/O per second to Target (Rolling Average)

Selects the array ports that match this parameter value.

**[-target-iops <integer>, ...]** - Number of IOPS to Target (Rolling Average)

Selects the array ports that match this parameter value.

**[-target-lun-in-use-count <integer>, ...]** - Target LUN In Use Count

Selects the array ports that match this parameter value (number of IN-USE disks on this target port).

**[-target-port-speed <text>]** - Target Port Speed

Selects the array ports that match this parameter value (speed that the target port has negotiated with its connected switch port, or initiator port if direct attached).

## Examples

The example below displays the port information for a single port.

```
cluster1::> storage array port show -wwpn 50060e80004291c0
Array Name: HITACHI_DF600F_1
WWNN: 50060e80004291c0
```

---

WWPN: 50060e80004291c0  
Connection Type: fabric  
Switch Port: vgb300s89:9  
Link Speed: 4 GB/s  
Max Queue Depth: 1024

Node	Initiator	LUN Count	IOPS	KB/s	%busy	%waiting	Link Errs
vnv3070f20a	0b	2	0	0	0	0	0
vnv3070f20b	0b	2	0	0	0	0	0

---

## storage disk assign

Assign ownership of a disk to a system

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

### Description

The `storage disk assign` command is used to assign ownership of an unowned disk or array LUN to a specific node. You can also use this command to change the ownership of a disk or an array LUN to another node. You can designate disk ownership by specifying disk names, array LUN names, wildcards, or all (for all disks or array LUNs visible to the node). For disks, you can also set up disk ownership autoassignment. You can also assign disks to a particular pool.

### Parameters

{ **[-disk <disk path name>]** - Disk Path

This specifies the disk or array LUN that is to be assigned. Disk names take one of the following forms:

- Disks that are not attached to a switch are named in the form `<node>:<host_adapter>.<loop_ID>`. For array LUNs, the form is `<node>:<host_adapter>.<loop_ID>L<LUN>`. For instance, disk number 16 on host adapter 1a on a node named node0a is named node0a:1a.16. The same disk on LUN lun0 is named node0a:1a.16Llun0.
- Disks that are attached to a switch are named in the form `<node>:<switch_name>:<switch_port>.<loop_ID>`. For array LUNs, the form is `<node>:<switch_name>:<switch_port>.<loop_ID>L<LUN>`. For instance, disk number 08 on port 11 of switch fc1 on a node named node0a is named node0a:fc1:11.08. The same disk on LUN lun1 is named node0a:fc1:11.08Llun1.

The same disk or array LUN can have multiple names, depending on how the disk or array LUN is connected. For example, a disk known to a node named alpha as alpha:1a.19 can be known to a node named beta as beta:0b.37. All names are listed in the output of queries and are equally valid. To determine the unique identity of a disk or an array LUN, run a detailed query and look for the universal unique identifier (UUID) or serial number of the disk or array LUN.

---

A subset of disks or array LUNs can be assigned using the wildcard character (\*) in the `-disk` parameter. Either the `-owner` or the `-sysid` parameter must be specified with the `-disk` parameter. Do not use the `-node` parameter with the `-disk` parameter.

| **-all** [true] - Assign All Disks

This optional parameter causes all visible unowned disks or array LUNs to be assigned to the node specified in the `-node` parameter. The `-node` parameter must be specified with the `-all` parameter. Do not use the `-owner` or the `-sysid` parameter with the `-all` parameter.

| **[-type | -T** {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SATA | SSD}] - Storage Type

This optional parameter assigns ownership of a specific type of disk or array LUN (or a set of disks/array LUNs) to a node. The `-count` parameter must be specified with the `-type` parameter.

**-count** | **-n** <integer> - Disk Count

This optional parameter assigns ownership of a number of disks or array LUNs specified in the `-count` parameter, to a node.

| **-auto** [true] } - Auto Assign

This optional parameter causes all visible disks eligible for autoassignment to be immediately assigned to the node specified in the `-node` parameter, irregardless of the setting of the `disk.auto_assign` option. Only unowned disks on loops or stacks owned wholly by that system and which have the same pool information will be assigned.

The `-node` parameter must be specified with the `-auto` parameter. Do not use the `-owner` or the `-sysid` parameter with the `-auto` parameter. When possible, use `-auto` parameter rather than `-all` parameter to conform to disk ownership best practices. The `-auto` parameter is ignored for array LUNs.

**[-pool | -p** <integer>] - Pool

This optional parameter specifies the pool to which a disk must be assigned. It can take values of `Pool0` or `Pool1`.

**[-owner | -o** <nodename>] - Owner Name

This optional parameter specifies the node to which the disk or array LUN has to be assigned.

**[-sysid | -s** <nvrleid>] - New Owner ID

This optional parameter specifies the serial number (NVRAM ID) of the node to which the disk or array LUN has to be assigned.

**[-checksum | -c** {block|zoned}] - Checksum Compatibility

---

This optional parameter is used to specify the checksum type for a disk or an array LUN. The possible values are block or zoned. Data ONTAP 8.1.1 supports a new checksum scheme called advanced zoned checksum (AZCS). Existing zoned checksum aggregates are still supported. A newly created aggregate with zoned checksum array LUNs is assigned AZCS checksum type. AZCS checksum type provides more functionality than the "version 1" zoned checksum type which has been supported in previous Data ONTAP releases. Zoned checksum spare array LUNs added to an existing zoned checksum aggregate continue to be zoned checksum. Zoned checksum spare array LUNs added to an AZCS checksum type aggregate use the AZCS checksum scheme for managing checksums. For some disks (e.g. FCAL, SSD, SAS disks), the checksum type cannot be modified. For more information on modifying the checksum type, refer to the "Physical Storage Management Guide".

**[-force | -f [true]]** - Force Flag

This optional parameter forces the assignment of ownership of an already owned disk to a node. This parameter could also be used to assign an array LUN with a redundancy error, for example, if the array LUN is available on only one path. For a disk which is part of a live aggregate, even specification of the `-force` parameter would not force the assignment, since it would be catastrophic.

**[-node | -N <nodename>]** - Node Name (For Auto Assign)

This optional parameter is used with either the `-auto` or the `-all` parameter. If used with the `-auto` parameter, all disks which are visible to the node specified in the `-node` parameter and which are eligible for autoassignment would be assigned to it. If used with the `-all` parameter, all unowned disks or array LUNs visible to the node would be assigned to it.

## Examples

The following example assigns ownership of an unowned disk named node0:1a.16 to a node named node1:

```
cluster1::> storage disk assign -disk node0:1a.16 -owner node1
```

The following example assigns all unowned disks or array LUNs visible to a node named node1 to itself:

```
cluster1::> storage disk assign -all -node node1
```

The following example autoassigns all unowned disks (eligible for autoassignment) visible to a node named node1 to itself:

```
cluster1::> storage disk assign -auto -node node1
```

The following two examples show the working of the `-force` parameter with a spare disk that is already owned by another system:

```
cluster1::> storage disk assign -disk node0:1a.16 -owner node1
Error: command failed: Failed to assign disks. Reason: Disk 1a.16 is
```

---

already owned.

```
cluster1::> storage disk assign -disk node0:1a.16 -owner node1 -force
Success.
```

The following example assigns ownership of the set of unowned disks connected to <host\_adapter> 1a of a node named node0, to a node named node1:

```
cluster1::> storage disk assign -disk node0:1a.* -owner node1
```

## storage disk fail

Fail the file system disk

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

### Description

The `storage disk fail` command can be used to manually force a file system disk to fail. It is used to remove a file system disk that may be logging excessive errors and requires replacement. To unfail a disk, use the `storage disk unfail` command.

### Parameters

**-disk** <disk path name> - Disk Name

This parameter specifies the disk to be failed.

**[-immediate | -i [true]]** - Fail immediately

This parameter optionally specifies whether the disk is to be failed immediately. It is used to avoid Rapid RAID Recovery and remove the disk from the RAID configuration immediately. Note that when a file system disk has been removed in this manner, the RAID group to which the disk belongs enters degraded mode (meaning a disk is missing from the RAID group). If a suitable spare disk is available, the contents of the disk being removed are reconstructed onto that spare disk.

### Examples

The following example fails a disk named node0:1a.16 immediately:

```
cluster1::> storage disk fail -disk node0:1a.16 -i true
WARNING: The system will not prefail the disk and its contents will not be
copied to a replacement disk before being failed out. Do you want to
fail out the disk immediately? {y|n}: y
```

### See Also



---

storage disk unfail

---

## storage disk modify

Modify disk attributes

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

### Description

The `storage disk modify` command can be used to modify the owner of a disk, a disk's state, or both. The command typically prompts you for confirmation of certain operations; if confirmation messages are disabled, the command attempts to force the operation. To fail a disk, use the `storage disk fail` command.

### Parameters

**-disk** <disk path name> - Disk Name

This specifies the disk that is to be modified. Disk names take one of the following forms:

- Disks that are not attached to a switch are named in the form <node>:<host\_adapter>.<loop\_ID>. For disks with a LUN, the form is <node>:<host\_adapter>.<loop\_ID>L<LUN>. For instance, disk number 16 on host adapter 1a on a node named node0a is named node0a:1a.16. The same disk on LUN lun0 is named node0a:1a.16Llun0.
- Disks that are attached to a switch are named in the form <node>:<switch\_name>:<switch\_port>.<loop\_ID>. For disks with a LUN, the form is <node>:<switch\_name>:<switch\_port>.<loop\_ID>L<LUN>. For instance, disk number 08 on port 11 of switch fc1 on a node named node0a is named node0a:fc1:11.08. The same disk on LUN lun1 is named node0a:fc1:11.08Llun1.

The same disk can have multiple disk names, depending on how the disk is connected. For example, a disk known to a node named alpha as alpha:1a.19 can be known to a node named beta as beta:0b.37. All names are listed in the output of queries and are equally valid. To determine a disk's unique identity, run a detailed query and look for the disk's universal unique identifier (UUID) or serial number.

**[-force-owner [true]]** - Force Flag

This parameter may be used to forcibly modify disk ownership in the following cases: a disk already has an assigned owner, there are disk errors such as a single-pathed disk or the disk is connected to a single controller. Using this parameter will not force the

---

change in cases where it would result in catastrophic data loss. This would be the case when a disk is part of a live aggregate, for example. This parameter defaults to true.

**[-owner {<nodename>|local}]** - Owner

This optionally specifies the node that owns the disk.

**[-owner-id <nvr amid>]** - Owner System ID

This optional parameter specifies the serial number (NVRAM ID) of the node that owns the disk.

**[-state {broken | copy | maintenance | partner | pending | present | reconstructing | removed | spare | unfail | zeroing}]** - State

This optionally specifies the disk's state. Possible values include the following:

- spare - This sets the disk as a spare for its RAID group
- broken - This marks that the disk is broken
- removed - This indicates that the disk has been removed from its disk shelf
- unfail - This removes the failed indication from the disk

## Examples

The following example does not allow the owner of an already assigned disk named node0:1a.16 to be modified from node0 to node1:

```
cluster1::> storage disk modify -disk node0:1a.16 -owner node1
Error: command failed: Failed to change the owner of disk node0:1a.16. Reason:
Disk node0:1a.16 is already owned.
```

But the following example changes the owner of the disk node0:1a.16 from node0 to node1, using the force-owner parameter:

```
cluster1::> storage disk modify -disk node0:1a.16 -owner node1 -force-owner
```

The following example does not allow the owner of an unassigned disk named node0:1a.20 to be modified to node1, if the disk has a single point of fault (such as the disk having only a single path, or the disk being connected to only one controller):

```
cluster1::> storage disk modify -disk node0:1a.20 -owner node1
Error: command failed: Failed to change the owner of disk node0:1a.20. Reason:
Storage disk modify failed: Redundancy errors were detected on disk
node0:1a.20 and force option not specified.
Use 'storage errors show' for detailed information.
```

But the following example changes the owner of the unassigned disk node0:1a.20 to node1 using the -force-owner parameter, even if the disk has a single point of fault:

```
cluster1::> storage disk modify -disk node0:1a.20 -owner node1 -force-owner
```

## See Also

storage disk fail

---

## storage disk reassign

Change the default owner of all disks from one node to another

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

### Description

The `storage disk reassign` command changes the ownership of all disks on a node to the ownership of another node. Use this command only when a node has a complete failure (for instance, a motherboard failure) and is replaced by another node. If the node's disks have already been taken over by its storage failover partner, use the `-force` parameter.

### Parameters

{ **-home** | **-o** {<nodename>|local} } - Current Home Name

This optionally specifies the name of the failed node. If you do not specify this parameter, you must specify the `-homeid` parameter instead.

| **-homeid** | **-s** <nvrleid> } - Current Home ID

This optionally specifies the serial number of the failed node. If you do not specify this parameter, you must specify the `-home` parameter instead.

{ **-newhome** | **-n** <text> } - New Home Name

This optionally specifies the name of the node that is to take ownership of the failed node's disks. If you do not specify this parameter, you must specify the `-newhomeid` parameter instead.

| **-newhomeid** | **-d** <nvrleid> } - New Home ID

This optionally specifies the serial number of the node that is to take ownership of the failed node's disks. If you do not specify this parameter, you must specify the `-newhome` parameter instead.

[**-force** | **-f** [true]] - Force

This optionally specifies whether to force the reassignment operation. The default setting is `false`.

### Examples

---

In the following example, a node named node0 has failed. Its disks have been not taken over by its storage failover partner. A replacement node with serial number 23456789 has been installed and connected to node0's disk shelves. To assign node0's disks to the new node, start the new node and run the following command:

```
node::*> storage disk reassign -home node0 -newhomeid 23456789
node0:1a.11, node0:1a.12, node0:1a.13, node0:1a.14,
node0:1a.15, node0:1a.16, node0:1a.23 and node0:1a.24
were reassigned to new owner with serial number 23456789.
```

In the following example, a similar failure has occurred, except that node0's disks have been taken over by its storage failover partner, node1. A new node, node5, has been installed and configured. To assign the disks that previously belonged to node0 to node5, run the following commands:

```
node::*> storage disk reassign -home node0 -newhome node5 -force true
node0:1a.11, node0:1a.12, node0:1a.13, node0:1a.14,
node0:1a.15, node0:1a.16, node0:1a.23 and node0:1a.24
were reassigned to new owner node5.
```

---

## storage disk remove

Remove a spare disk

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

### Description

The `storage disk remove` command removes the specified spare disk from the RAID configuration, spinning the disk down when removal is complete.

This command does not remove disk ownership information from the disk. Therefore, if you plan to reuse the disk in a different storage system, you should use the `storage disk removeowner` command instead. See the "Physical Storage Management Guide" for the complete procedure.

NOTE: For systems with multi-disk carriers, it is important to ensure that none of the disks in the carrier are filesystem disks before attempting removal. To convert a filesystem disk to a spare disk, see `storage disk replace`.

### Parameters

**-disk** <disk path name> - Disk Name

This parameter specifies the disk to be removed.

### Examples

The following example removes a spare disk named node0:1a.16:

```
cluster1::> storage disk remove -disk node0:1a.16
```

### See Also

`storage disk removeowner`   `storage disk replace`

---

## storage disk removeowner

Remove disk ownership

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

### Description

The `storage disk removeowner` command removes ownership from a specified disk. Then disk can then be reassigned to a new owner.

### Parameters

**-disk** <disk path name> - Disk Name

This specifies the disk whose ownership is to be removed.

**[-force [true]]** - Force the Ownership Removal

This option tells ONTAP to override the normal restriction preventing the removal of spare disks. For disks which are part of a live aggregate, even specification of force parameter would not force the disk ownership removal, since it would be catastrophic.

### Examples

The following example removes the ownership from a disk named node1:0c.27.

```
cluster1::> storage disk removeowner -disk node1:0c.27
```

## storage disk replace

Initiate or stop replacing a file-system disk

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

### Description

The `storage disk replace` command starts or stops the replacement of a file system disk with spare disk. When you start a replacement, Rapid RAID Recovery begins copying data from the specified file system disk to a spare disk. When the process is complete, the spare disk becomes the active file system disk and the file

---

system disk becomes a spare disk. If you stop a replacement, the data copy is halted, and the file system disk and spare disk retain their initial roles.

## Parameters

**-disk** <disk path name> - Disk Name

This specifies the file system disk that is to be replaced. See the documentation for the `storage disk modify` command for information on disk-naming conventions.

**-action** {start|stop} - Action

This specifies whether to start or stop the replacement process.

**[-replacement** <disk path name>] - Replacement

This specifies the spare disk that is to replace the file system disk.

**[-allow-same-carrier** [true]] - Allow Same RAID Group Within Carrier

This parameter can be used to allow two disks housed in the same carrier to be in the same RAID group when you replace a disk in an aggregate.

Having disks in the same carrier in the same RAID group is not desirable because a carrier failure can cause a simultaneous outage for two disks in the same RAID group. You can replace a disk in an aggregate with a disk that causes this situation, but when an alternate disk becomes available, Data ONTAP automatically initiates a series of disk copy operations to put the disks into different RAID groups. For this reason, you should use this parameter only when necessary. When possible, ensure that disks housed in the same carrier are in different RAID groups.

This parameter affects only the disk replace operation. It is not a persistent attribute of the aggregate.

**[-allow-mixing | -m** [true]] - Allow Mixing of Disks of Different RPM or Pool

This optional parameter specifies whether the disk can be replaced with another disk of different RPM or from different Pool. This parameter affects only the current disk replacement operation.

## Examples

The following example begins replacing a file system disk named `node0:1a.16` with a spare disk named `node0:1b.14`.

```
cluster1::> storage disk replace -disk node0:1a.16 -replacement node0:1b.14 -  
action start
```

## See Also



---

storage disk modify

---

## storage disk set-led

Turn on a disk's red LED for a number of minutes

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

### Description

The `storage disk set-led` controls the LED of a specified disk.

You can turn an LED on or off, cause it to blink or stop blinking, or test it.

This command is useful for locating a disk in its shelf.

### Parameters

**-disk** <disk path name> - Disk Name

This specifies the disk whose LED is to be set.

See the documentation for the `storage disk modify` command for information on disk-naming conventions.

**-action** {on|off|blink|blinkoff|test} - Action

This specifies the state to which the LED is to be set. Possible values include the following:

- on-The LED lights up steadily
- off-The LED does not light up
- blink-The LED blinks
- blinkoff-The LED stops blinking
- test-This tests the operation of the disk enclosure's hardware and drivers. Do not use this value in normal operation.

**[-time <integer>]** - Time (Min)

This specifies the time, in minutes, that the LED is to remain in the specified state.

### Examples

The following example causes the LEDs on all disks whose names match the pattern `Cluster1*` to turn on:

---

```
Cluster1::> storage disk set-led -disk Cluster1* -action on
```

## **See Also**

storage disk modify

---

## storage disk show

Display a list of disk drives and array LUNs

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

### Description

The `storage disk show` command displays information about disks and array LUNs. Where it appears in the remainder of this document "disk" may refer to either a disk or an array LUN. By default, the command displays the following information about all disks in column style output:

- Disk name
- Usable space on the disk, in human readable units
- Shelf number
- Bay number
- Container type (aggregate, broken, foreign, labelmaint, maintenance, spare, unassigned, unknown, or volume)
- Position (copy, data, dparity, orphan, parity, pending, or present)
- Aggregate name
- Owning node name

To display detailed information about a single disk, use the `-disk` parameter.

### Parameters

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

Displays the specified fields for all disks, in column style output.

| **[-broken]**

Displays the following RAID-related information about broken disks:

- Original owning node name
- Checksum compatibility
- Disk name

- 
- Outage reason
  - Host bus adapter
  - Shelf number
  - Bay number
  - Primary port / Channel
  - Pool
  - Disk type
  - RPM (Revolutions per minute)
  - Usable size in human readable units
  - Physical size in human readable units
  - Current owner node

#### | [-longop ]

Displays the following information about long-running disk operations, in column style output:

- Disk name
- Whether the disk is marked as prefailed
- Whether the disk is being replaced
- Whether the disk is zeroed
- Copy destination
- Percentage of copy complete
- Percentage of zeroing complete
- Percentage of reconstruction complete

#### | [-maintenance ]

Displays the following RAID-related information about disks in the maintenance center:

- Original owning node name
- Checksum compatibility
- Disk name
- Outage Reason

- 
- Host bus adapter
  - Shelf number
  - Bay number
  - Primary port / Channel
  - Pool
  - Disk type
  - RPM (Revolutions per minute)
  - Usable size in human readable units
  - Physical size in human readable units
  - Current owner node

#### | [-ownership ]

Displays the following ownership-related information:

- Disk name
- Aggregate name
- Home node name
- Owning node name
- Disaster recovery home node name
- Home node system id
- Owning node system id
- Disaster recovery home node system id
- Reservation node system id

#### | [-physical ]

Displays the following information about the disk's physical attributes, in column style output:

- Disk name
- Disk type
- Disk vendor
- Disk model

- 
- Firmware revision level
  - RPM (Revolutions per minute)
  - BPS (Bytes per sector)

#### | [-port ]

Displays the following path-related information:

- Disk name and disk port associated with disk primary path
- Disk name and disk port associated with the disk secondary path, for a multipath configuration
- Type, shelf, and bay information for the disks

#### | [-raid ]

Displays the following RAID-related information:

- Disk name
- Container type (aggregate, broken, labelmaint, maintenance, spare, unassigned, unknown, or volume)
- Outage reason
- Position (copy, data, dparity, orphan, parity, pending, or present)
- RAID group name
- Aggregate name

#### | [-raid-info-for-aggregate ]

Displays the following RAID-related information about the disks used in an aggregate:

- Owning node name
- Aggregate name
- Plex name
- RAID group name
- Position (copy, data, dparity, orphan, parity, pending, or present)
- Disk name
- Host bus adapter
- Shelf number

- 
- Bay number
  - Primary port / Channel
  - Pool
  - Disk type
  - RPM (Revolutions per minute)
  - Usable size in human readable units
  - Physical size in human readable units

| **[-spare]**

Displays the following RAID-related information about available spare disks:

- Original owning node name
- Checksum compatibility
- Disk name
- Host bus adapter
- Shelf number
- Bay number
- Primary port / Channel
- Pool
- Disk type
- RPM (Revolutions per minute)
- Usable size in human readable units
- Physical size in human readable units
- Current owner node

| **[-instance]** }

Displays detailed disk information. If no disk path name is specified, this parameter displays the same detailed information for all disks as does the -disk parameter. If a disk path name is specified, then this parameter displays the same detailed information for the specified disks as does the -disk parameter.

**[-disk <disk path name>]** - Disk Name



---

Displays detailed information about the specified disks. See `storage disk modify` for information about disk-naming conventions.

**[-owner {<nodename>|local}]** - Owner

Selects information about disks that are owned by the specified node.

**[-owner-id <nvramid>]** - Owner System ID

Selects the disks that are owned by the node with the specified system ID.

**[-state {broken | copy | maintenance | partner | pending | present | reconstructing | removed | spare | unfail | zeroing}]** - State

Displays the old-style RAID state of the disk. This parameter will be deprecated in a future release. To determine the basic RAID disposition of a disk, use the `-container-type` and `-position` fields.

**[-uid <text>]** - Disk Unique ID

Selects the disks whose unique id matches this parameter value. A disk unique identifier has the form:

20000000:875D4C32:00000000:00000000:00000000:00000000:00000000:00000000:00000000:00000000

**[-aggregate <aggregate name>]** - Aggregate

Selects information about disks that belong to the specified aggregate.

**[-array-name <array name>]** - Array Name

Selects information about the LUNs presented by the specified storage array.

**[-average-latency <integer>]** - Average I/O Latency Across All Active Paths

Selects information about disks that have the specified average latency.

**[-bay <integer>]** - Bay

Selects information about disks that are located in the carrier within the specified shelf bay.

**[-bps <integer>]** - Bytes Per Sector

Selects information about disks that have the specified number of bytes per sector. Possible settings are 512, 520, 4096, and 4160.

**[-carrier-id <text>]** - Carrier ID

Selects information about disks that are located within the specified multi-disk carrier.

**[-checksum-compatibility {advanced\_zoned | block | none | zoned/advanced\_zoned}]** - Checksum Compatibility

---

Selects information about disks that have the specified checksum compatibility.

**[-container-type {aggregate | broken | foreign | labelmaint | maintenance | spare | unassigned | unknown | volume}]** - Container Type

Selects information about disks that have the specified container type.

**[-copy-destination <disk path name>]** - Copy Destination Name

Selects information about disks whose contents are being copied (due to either Rapid RAID Recovery or disk replacement) to the specified spare disk.

**[-copy-percent <integer>]** - Percentage of Copy Complete

Selects information about disks that are involved as either a source or destination of a copy operation, (due to either disk replacement or Rapid RAID Recovery) and that have the specified percentage of the copy operation completed.

**[-disk-io-kbps-total <integer>]** - Total Disk Throughput in KBPS Across All Active Paths

Selects information about disks that have attained the specified I/O throughput on all connected paths.

**[-disk-iops-total <integer>]** - Total Disk IOPs Across All Active Paths

Selects information about disks that have achieved the specified number of IOPs per second on all connected paths.

**[-diskpathnames <disk path name>, ...]** - list of path based disk names

Selects information about disks that have all of the specified path names.

**[-effective-rpm <integer>]** - Effective RPM

Selects information about disks with the specified effective rotational speed.

**[-dr-home {<nodename>|local}]** - Disaster Recovery Home

Selects information about disks that have the specified Disaster home node.

**[-dr-home-id <nvrmaid>]** - Disaster Recovery Home System ID

Selects information about disks whose Disaster home node has the specified system id.

**[-errors <text>, ...]** - Error Text

Selects information about disks that have the specified error text.

**[-firmware-revision <text>]** - Firmware Revision

Selects information about disks that have the specified firmware revision level.

**[-home {<nodename>|local}]** - Home

---

Selects information about disks that have the specified home node.

**[-home-id <nvramid>]** - Home System ID

Selects information about disks whose home node has the specified system ID.

**[-host-adapter <text>]** - Primary Path Host Adapter

Selects information about disks that are currently using the specified Host Bus Adapter.

**[-import-in-progress {true|false}]** - Foreign LUN import in progress

Selects information about the array LUNs that are currently being imported

**[-initiator <text>, ...]** - Initiator Port

Selects information about disks that are visible to the initiator specified. Disks that are not currently in use by that initiator are included.

**[-initiator-iops <integer>, ...]** - Number of IOPS on Initiator (Rolling Average)

Selects information about disks that are visible to an initiator that has executed the specified number of IOPs.

**[-initiator-io-kbps <integer>, ...]** - Kbytes of I/O per second on Initiator (Rolling Average)

Selects information about disks visible to an initiator that has executed I/O at the specified throughput.

**[-initiator-lun-in-use-count <integer>, ...]** - Number of LUNs in the in-use state on this initiator

Selects information about disks with a path through an initiator that has the specified in-use-count.

**[-initiator-side-switch-port <text>, ...]** - Initiator Side Switch Port

Selects information about disks that are visible to an initiator connected to the specified switch port.

**[-is-multidisk-carrier {true|false}]** - Multi Disk Carrier?

Selects information about disks that are located within a multi-disk carrier.

**[-lun <integer>, ...]** - LUN ID

Selects information about the specified LUNs.

**[-lun-iops <integer>, ...]** - Number IOPS per second on disk (Rolling Average)

Selects information about the LUNs that have reached the specified number of IOPs.

**[-lun-io-kbps <integer>, ...]** - Kbytes/sec on Disk (Rolling Average)

---

Selects information about the LUNs that have reached the specified I/O throughput.

**[-lun-path-use-state <text>, ...]** - The Use State of the LUN on this path

Selects information about LUNs reporting the specified in-use state.

**[-model <text>]** - Model

Selects information about disks of the specified model.

**[-nodelist {<nodename>|local}, ...]** - Controller name

Selects information about disks that are visible to all of the specified nodes .

**[-outage-reason <text>]** - Outage Reason

Selects information about disks that are not in service for the specified reason.

Possible values are: admin failed, admin removed, admin testing, evacuated, bad label, bypassed, failed, init failed, label version, labeled broken, labelmaint, LUN resized, missing, not responding, predict failure, rawsize shrank, recovering, sanitizing, sanitized, SnapLock Disk, testing, unassigned, unknown.

**[-path-error-count <integer>]** - Path Error Count

Selects information about disks that are visible on a path that has incurred the specified number of errors.

**[-path-iops <integer>, ...]** - Number of IOPS on Path (Rolling Average)

Selects information about disks on those paths that have reached the specified number of IOPs.

**[-path-io-kbps <integer>, ...]** - Kbytes of I/O per second on Path (Rolling Average)

Selects information about disk with paths that have reached the specified I/O throughput

**[-path-link-errors <integer>, ...]** - Link Error count on path

Selects information about disks with paths that have incurred the specified number of FC link errors.

**[-path-lun-in-use-count <integer>, ...]** - Number of LUNs in the in-use state on this path

Selects information about disks with paths that have the specified in-use-count.

**[-path-quality <integer>, ...]** - Percentage of weighted error threshold

Selects information about disks on paths that have incurred the specified number of errors. The value displayed is a measure of the health of a path expressed as a percentage of an error threshold. Once a path has reached or surpassed the error threshold, another path will be selected for I/O transfer, if there is one available.

**[-physical-size-mb <integer>]** - Physical Size (MB)

---

Selects information about disks that have the specified physical capacity, in megabytes.

**[-physical-size {<integer>[KB|MB|GB|TB|PB]]** - Physical Size

Selects information about disks that have the specified physical capacity, in human readable units.

**[-physical-size-512b <integer>]** - Physical Size in Units of 512 Bytes

Selects information about disks that have the specified physical capacity, in 512-byte chunks. This parameter is present only for backwards compatibility with Data ONTAP 8.0.

**[-plex <text>]** - Plex Name

Selects information about disks that belong to the specified RAID plex.

**[-port-speed <text>, ...]** - Port Speed

Selects information about disks that are served by a Host Bus Adapter that is running at the specified port speed.

**[-position {copy | data | dparity | orphan | parity | pending | present}]** - Disk Position

Selects information about disks that have the specified position within their disk container.

**[-prefailed {true|false}]** - Marked for Rapid RAID Recovery?

Selects information about disks that match the specified parameter value indicating whether the disk is either awaiting or is in process of Rapid RAID Recovery.

**[-preferred-target-port {true|false}, ...]** - Whether or not target port group is preferred (privilege: advanced)

Selects information about disks that match the specified parameter value indicating whether the backing storage is ALUA (Assymmetric Logical Unit Access) capable and has specified the array target port on this path to be a preferred target port for I/O.

**[-primary-port <text>]** - Primary Path Disk Port

Selects information about disks that use the specified primary port.

**[-raid-group <text>]** - Raid Group Name

Selects information about disks that belong to the specified RAID group.

**[-reconstruction-percent <integer>]** - Percentage of Reconstruction Complete

Selects information about disks that are being reconstructed and that have the specified percentage of the reconstruction operation completed.

**[-replacing {true|false}]** - Being Replaced?

---

Selects information about disks that match the specified boolean value indicating whether the disk is either awaiting or in process of disk replacement.

**[-reserver-id <integer>]** - Reservation System ID

Selects information about disks that are reserved by the node with the specified system ID.

**[-rpm <integer>]** - Revolutions Per Minute

Selects information about disks that have the specified rotational speed.,

**[-secondary-name <disk path name>]** - Secondary Path Name

Selects information about disks that use the specified secondary path name, for multipath configuration.

**[-secondary-port <text>]** - Secondary Path Disk Port

Selects information about disks that use the specified secondary port.

**[-serial-number <text>]** - Serial Number

Selects information about the disk that has the specified serial number.

**[-shelf <integer>]** - Shelf

Selects information about disks that are located within the specified shelf.

**[-target-iops <integer>, ...]** - Number of IOPS to Target (Rolling Average)

Selects information about disks that are visible on target ports that have performed the specified number of IOPs.

**[-target-io-kbps <integer>, ...]** - Kbytes of I/O per second to Target (Rolling Average)

Selects information about disks that are visible on target ports that have reached the specified I/O throughput.

**[-target-lun-in-use-count <integer>, ...]** - Number of LUNs in the in-use state on this target

Selects information about disks with a path through a target port that has the specified in-use-count.

**[-target-port-access-state <text>, ...]** - Failover optimization type

Selects information about disks that are visible on target ports that have the specified access state.

**[-target-side-switch-port <text>, ...]** - Target Side Switch Port

---

Selects information about disks that are visible on target ports identified by the switch port to which they are connected.

**[-target-wwpn <text>, ...]** - Target Port

Selects information about disks that are visible on target ports identified by their World Wide Port Name.

**[-tpgn <integer>, ...]** - Target Port Group Number

Selects information about disks that belong to the specified Target Port Group Number.

**[-type {ATA | BSAS | EATA | FCAL | FSAS | LUN | MSATA | SAS | SATA | SCSI | SSD | XATA | XSAS}]** - Disk Type

Selects information about disks that have the specified disk type.

**[-usable-size-mb <integer>]** - Usable Size (MB)

Selects information about disks that have the specified usable space, in megabytes.

**[-usable-size [<integer>[KB|MB|GB|TB|PB]]]** - Usable Size

Selects information about disks that have the specified usable space, in human readable units.

**[-vendor <text>]** - Vendor Name

Selects information about disks that have the specified usable space, in human readable units.

**[-zeroed {true|false}]** - Zeroed?

Selects information about disks that have (true) or have not (false) been fully pre-zeroed.

**[-zeroing-percent <integer>]** - Percentage of Zeroing Complete

Selects information about disks that are zeroing and have the specified percentage complete.

## Examples

The following example displays information about all disks:

```
cluster1:>> storage disk show
```

Disk	Usable Size	Shelf	Bay	Container Type	Position	Aggregate	Owner
node1:0a.17	10GB	1	1	spare	present	-	node1
node1:0a.20	78.59GB	1	4	spare	present	-	node1
node1:0a.28	10GB	1	12	spare	present	-	node1
node1:0a.44	10GB	2	12	broken	present	-	node1
node1:0a.55	78.59GB	3	7	aggregate	parity	aggr0_u23	node1
node1:0b.22	78.59GB	1	6	broken	present	-	node1
node1:0b.42	78.59GB	2	10	aggregate	dparity	aggr0_u23	node1

node1:0b.73	78.59GB	4	9	aggregate	data	aggr0_u23	node1
node2:0c.16	10GB	1	0	aggregate	dparity	aggr0_u22	node2
node2:0c.17	10GB	1	1	aggregate	data	dp_degraded	node2
node2:0c.18	10GB	1	2	spare	present	-	node2
node2:0c.19	20GB	1	3	spare	present	-	node2
node2:0c.20	20GB	1	4	spare	present	-	node2
node2:0c.22	10GB	1	6	aggregate	data	dp_sdc	node2
node2:0d.21	268.0GB	1	5	maintenance	present	-	node2
node2:0d.48	10GB	3	0	aggregate	parity	aggr0_u22	node2
node2:0d.75	10GB	4	11	spare	present	-	node2
node2:0d.77	20GB	4	13	broken	present	-	node2
[...]							

The following example displays detailed information about a disk named node2:0d.75

```
cluster1::> storage disk show -disk node2:0d.75
Disk: node2:0d.75
Container Type: spare
Owner/Home: node2 / node2
DR Home:
Array: N/A
Vendor: VENDOR
Model: X267_HKURO500SSX
Serial Number: ZAKAS0GH
UID:
1FF17846:0A419201:9325845A:3ABD5075:00000000:00000000:00000000:00000000:00000000:00000000
BPS: 512
Physical Size: 10.15GB
Position: present
Checksum Compatibility: block
Aggregate: -
Plex: -

Paths:
Controller      Initiator      LUN  Initiator Side      Target Side
Acc Use Target Port      ID  Switch Port      I/O KB/s      IOPS
-----
node1
AO INU 220a000a3384e4d2 0 N/A 21 2 Gb/s N/A 0 0
node1
AO RDY 2209000a3384e4d2 0 N/A 62 2 Gb/s N/A 0 0
node2
AO INU 2209000a3384e4d2 0 N/A 62 2 Gb/s N/A 3 0

Errors:
-
```

The following example displays RAID-related information about disks used in an aggregate:

```
cluster1::> storage disk show -raid-info-for-aggregate
Owner Node: node1
Aggregate: aggr0_node1_0
Plex: plex0
RAID Group: rg0

Usable Physical      HA Shelf Bay Chan Pool  Type  RPM
Size      Position Size
-----
9.77GB    data      node1:2d.11.2    2d    11    2 B    Pool0  SAS  15000
9.93GB    dparity   node1:2d.11.0    2d    11    0 B    Pool0  SAS  15000
9.77GB    parity    node1:2d.11.1    2d    11    1 B    Pool0  SAS  15000
9.93GB    parity    node1:2d.11.1    2d    11    1 B    Pool0  SAS  15000
Owner Node: node2
Aggregate: al
Plex: plex0
RAID Group: rg0

Usable Physical      HA Shelf Bay Chan Pool  Type  RPM
Size      Position Size
-----
```



```

-----
9.77GB data node2:2a.01.8 2a 1 8 B Pool0 BSAS 7200
9.91GB dparity node2:2a.01.6 2a 1 6 B Pool0 BSAS 7200
9.77GB 9.91GB parity node2:2a.01.7 2a 1 7 B Pool0 BSAS 7200
9.77GB 9.91GB
Owner Node: node2
Aggregate: al
Plex: plex0
RAID Group: rg1

```

```

Usable Physical
Size Position Disk HA Shelf Bay Chan Pool Type RPM
-----
9.77GB data node2:2a.01.11 2a 1 11 B Pool0 BSAS 7200
9.91GB dparity node2:2a.01.9 2a 1 9 B Pool0 BSAS 7200
9.77GB 9.91GB parity node2:2a.01.10 2a 1 10 B Pool0 BSAS 7200
9.77GB 9.91GB
Owner Node: node2
Aggregate: aggr0
Plex: plex0
RAID Group: rg0

```

```

Usable Physical
Size Position Disk HA Shelf Bay Chan Pool Type RPM
-----
9.71GB data node2:2a.01.5 2a 1 5 B Pool0 BSAS 7200
10.03GB dparity node2:2a.01.2 2a 1 2 B Pool0 BSAS 7200
9.71GB 10.03GB parity node2:2a.01.4 2a 1 4 B Pool0 BSAS 7200
9.71GB 10.03GB
12 entries were displayed.

```

The following example displays RAID-related information about spares:

```

cluster1::> storage disk show -spare
Original Owner: node1
Checksum Compatibility: block
Disk HA Shelf Bay Chan Pool Type RPM Usable Physical Owner
-----
node1:0b.23 0b 1 7 A Pool0 FCAL 10000 132.8GB 134.2GB node1
node1:0b.25 0b 1 9 A Pool0 FCAL 10000 132.8GB 133.9GB node1
node1:0b.26 0b 1 10 A Pool11 FCAL 10000 132.8GB 133.9GB node1
node1:0b.27 0b 1 11 A Pool11 FCAL 10000 132.8GB 134.2GB node1
Home Owner: node2
Checksum Compatibility: block
Disk HA Shelf Bay Chan Pool Type RPM Usable Physical Owner
-----
node2:0a.19 0a 1 3 B Pool11 FCAL 10000 132.8GB 133.9GB node2
node2:0a.20 0a 1 4 B Pool0 FCAL 10000 132.8GB 133.9GB node2
node2:0a.21 0a 1 5 B Pool0 FCAL 10000 132.8GB 133.9GB node2
[...]
```

The following example displays RAID-related information about broken disks:

```

cluster1::> storage disk show -broken
Original Owner: node1
Checksum Compatibility: block
Physical Disk Outage Reason HA Shelf Bay Chan Pool Type RPM Usable
Size
-----
```

```

node1:0b.16      admin failed 0b      1    0    A Pool0 FCAL  10000 132.8GB
133.9GB
node1:0b.38      admin removed 0b      2    6    A Pool1 FCAL  10000 132.8GB
134.2GB
Original Owner: node2
Checksum Compatibility: block
Usable
Physical
Disk      Outage Reason HA Shelf Bay Chan  Pool  Type    RPM    Size
Size
-----
node2:0a.16      admin failed 0a      1    0    B Pool0 FCAL  10000 132.8GB
133.9GB
node2:0a.29      admin removed 0a      1   13    B Pool0 FCAL  10000 132.8GB
133.9GB
4 entries were displayed.

```

The following example displays RAID-related information about disks in maintenance center:

```

cluster1:>> storage disk show -maintenance
Original Owner: node1
Checksum Compatibility: block
Usable
Physical
Disk      Outage Reason HA Shelf Bay Chan  Pool  Type    RPM    Size
Size
-----
node1:0b.24      admin testing 0b      1    8    A Pool0 FCAL  10000 132.8GB
133.9GB
node1:0b.43      admin testing 0b      2   11    A Pool1 FCAL  10000 132.8GB
134.2GB
Original Owner: node2
Checksum Compatibility: block
Usable
Physical
Disk      Outage Reason HA Shelf Bay Chan  Pool  Type    RPM    Size
Size
-----
node2:0a.42      admin testing 0a      2   10    B Pool1 FCAL  10000 132.8GB
133.9GB
node2:0a.45      admin testing 0a      2   13    B Pool1 FCAL  10000 132.8GB
134.2GB
4 entries were displayed.

```

## See Also

storage disk modify

---

## storage disk unfail

Unfail a broken disk

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

### Description

The `storage disk unfail` command can be used to unfail a broken disk.

If the `-s` option is used, the disk is returned to the spare pool upon unfail. Otherwise, the disk is brought back into its parent aggregate. This may result in the aggregate coming back online if it is not complete or online at that time.

If the attempt to unfail the disk is unsuccessful, the disk remains in broken state.

### Parameters

**-disk** <disk path name> - Disk Name

This parameter specifies the disk to be unfailed.

**[-s [true]]** - Make the disk spare

This parameter specifies whether the unfailed disk will be made a spare disk. The disk is forced to become a spare disk if this is true. Default value is false.

### Examples

The following example unfails a disk named `node0:1a.16` to become a spare disk:

```
cluster1::*> storage disk unfail -disk node0:1a.16 -s true
```

## storage disk updatefirmware

Update disk firmware

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

### Description

---

The `storage disk updatefirmware` command updates the firmware on one or more disks.

You can download the latest firmware by using the `storage firmware download` command.

You can specify a list of one or more disks whose firmware is to be updated by using the `-disk`

parameter, or you can update the firmware on all local disks by omitting the `-disk` parameter.

## Parameters

`[-disk <disk path name>, ...]` - Disk

This specifies the disk or disks whose firmware is to be updated.

If you do not specify this option, all local disks' firmware is updated.

## Examples

The following example updates the firmware on all disks:

```
Cluster1::> storage disk updatefirmware
```

## See Also

[storage firmware download](#)

---

## storage disk zerospares

Zero non-zeroed spare disks

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

### Description

The `storage disk zerospares` command zeroes all non-zeroed spare disks in all nodes or a specified node in the cluster. A node must be online to zero disks. Zeroing a disk writes zeros to the entire disk and must be done before a disk can be reused in another aggregate.

### Parameters

`[-owner {<nodename>|local}]` - Owner

If this parameter is specified, only non-zeroed spares assigned to the specified node will be zeroed. Otherwise, all non-zeroed spares in the cluster will be zeroed.

### Examples

The following example zeroes all non-zeroed spares owned by a node named node4:

```
cluster1::> storage disk zerospares -owner node4
```

## storage disk option modify

Modify disk options

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

### Description

The `storage disk option modify` command modifies the background firmware update setting, automatic copy setting, automatic disk assignment of all disks assigned to a specified node, or modifies the setting of automatic disk assignment of unowned disks at a shelf level granularity.

### Parameters

---

**-node** {<nodename>|local} - Node

This parameter specifies the node that owns the disks whose options are to be modified.

**[-bkg-firmware-update** {on|off}] - Background Firmware Update

This parameter specifies whether firmware updates run as a background process. The default setting is `on`, which specifies that firmware updates to spare disks and file system disks is performed nondisruptively via a background process. If the option is turned off, automatic firmware updates occur at system startup or during disk insertion.

**[-autocopy** {on|off}] - Auto Copy

This parameter specifies whether data is to be automatically copied from a failing disk to a spare disk in the event of a predictive failure. The default setting is `on`. It is sometimes possible to predict a disk failure based on a pattern of recovered errors that have occurred. In such cases, the disk reports a predictive failure. If this option is set to `on`, the system initiates Rapid RAID Recovery to copy data from the failing disk to an available spare disk. When data is copied, the disk is marked as failed and placed in the pool of broken disks. If a spare is not available, the node continues to use the disk until it fails. If the option is set to `off`, the disk is immediately marked as failed and placed in the pool of broken disks. A spare is selected and data from the missing disk is reconstructed from other disks in the RAID group. The disk does not fail if the RAID group is already degraded or is being reconstructed. This ensures that a disk failure does not lead to the failure of the entire RAID group.

**[-autoassign** {on|off}] - Auto Assign

This parameter specifies whether automatic assignment of unowned disks is enabled or disabled. The default setting is `on`. When `on`, the default behavior is to automatically assign disks at the adapter (stack) level of granularity. If all assigned disks on an adapter (stack) have the same ownership assignment, and there are unowned disks present on that adapter (stack), automatic assignment will assign the unowned disks to match the ownership of the already assigned disks on that adapter (stack). This parameter is used to set both a node-specific and a cluster-wide disk option.

**[-autoassign-shelf** {on|off}] - Auto Assignment At Shelf Level

This parameter specifies whether automatic assignment of unowned disks should be done at the shelf level of granularity or not. This parameter is ignored if `autoassign` parameter is `off`. Otherwise, if both `autoassign` and `autoassign-shelf` parameters are `on`, then if there are unowned disks on a shelf and all assigned disks on that shelf have the same ownership assignment, automatic assignment will assign the unowned disks to match the ownership of the already assigned disks on that shelf. The default setting is `off`. This parameter is used to set both a node-specific and a cluster-wide disk option.

---

## Examples

The following example sets the background firmware update setting to on for all disks belonging to a node named node0:

```
cluster1::> storage disk option modify -node node0 -bkg-firmware-update on
```

## See Also

autoassign autoassign-shelf

---

## storage disk option show

Display a list of disk options

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

### Description

The `storage disk option show` command displays the settings of the following disk options:

- Background firmware update
- Automatic copying of data to a spare disk in the event of a predictive failure
- Automatic assignment of disks
- Automatic assignment of disks at a shelf level granularity

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the node that owns the disks.

[-**bkg-firmware-update** {on|off}] - Background Firmware Update

Selects the disks that match this parameter value.

[-**autocopy** {on|off}] - Auto Copy

Selects the disks that match this parameter value.

[-**autoassign** {on|off}] - Auto Assign

Selects the disks that match this parameter value.



---

**[-autoassign-shelf {on|off}] - Auto Assignment At Shelf Level**

Selects the disks that match this parameter value.

**Examples**

The following example displays disk-option settings for disks owned by all nodes in the cluster:

```
cluster1::> storage disk option show
Node      Bkg. FW. Upd.  Auto Copy  Auto Assign  Auto Assign Shelf
-----
node0      on              on          on           on
node1      on              on          on           on
node2      on              on          on           on
node3      on              on          on           on
4 entries were displayed.
```

---

## storage errors show

Display storage configuration errors.

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

### Description

The `storage errors show` command displays configuration errors with back end storage arrays.

### Parameters

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

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

| **[-instance ]** }

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

**[-uid <text>]** - UID

Selects the disks that match this parameter value.

**[-array-name <array name>]** - Array Name

Selects the disks that have the specified name for the storage array that is connected to the cluster.

**[-node {<nodename>|local}]** - Controller Name

Selects the disks that match this parameter value.

**[-disk <disk path name>]** - Disk

Selects the disks that match this parameter value.

**[-serial-number <text>]** - Serial Number

Selects the disks that match this parameter value.

**[-errors <text>, ...]** - Error Text

Selects the disks with display errors of the specified type.

---

**[-error-id <integer>, ...]** - Error ID

Selects the disks with error-id values that match this parameter value.

**[-error-type {onepath|onedomain|control|foreign|toobig|toosmall|invalidblocksize|targetasymmap|deviceasymmap|failovermisconfig|unknown|netapp}, ...]** - Error Type

Selects the disks with error types values that match this parameter value.

## Examples

The following example displays configuration errors seen in the system:

```
cluster1::> storage errors show
Disk: vnv3070f20b:vnci9124s54:1-24.126L23
-----
vnci9124s54:1-24.126L23 (600a0b800019e999000036b24bac3983): This array LUN
reports an invalid block size and is not usable. Only a block size of 512 is
supported.
```

---

## storage failover giveback

Return failed-over storage to its home node

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

### Description

The `storage failover giveback` command returns storage that has failed over to a node's partner back to the home node. This operation fails if other resource-intensive operations (for instance, system dumps) are running and make the giveback operation potentially dangerous or disruptive. Run the `storage failover show-giveback` command to check the status of giveback operations.

Note:

- If the system ID of the partner has changed while the node is in takeover mode, the `storage failover giveback` command updates the ownership of the partner's disks to the new system ID while giving back.
- If the giveback operation fails due to the operation being vetoed by a subsystem, check the syslog or EMS output for a subsystem-specific reason for the abort. The corrective action is subsystem-specific and is detailed in the corrective action portion of the message. Follow the corrective action specified by the subsystem and then reissue the `storage failover giveback` command. If you cannot perform the corrective action, then use the `override-vetoes` option in the `storage failover giveback` command to force the giveback.
- If the giveback operation fails because the node cannot communicate with its partner, check the EMS output for the corrective action. Follow the corrective action and then reissue the `storage failover giveback` command. If you cannot perform the corrective action, then use the `-require-partner-waiting false` option in the `storage failover giveback` command to force the giveback.
- If the node does not receive notification that the partner has brought online the given-back aggregate and its volumes, the `storage failover show-giveback` command displays the giveback status for the aggregate as failed. A possible reason for this failure is that the partner is overloaded and slow in bringing the aggregate online. Run the `storage aggregate show` command to verify that the aggregate and its volumes are online on the partner node. The node will not attempt the giveback operation for remaining aggregates. To force

---

the giveback, use the `-require-partner-waiting false` option in the `storage failover giveback` command.

## Parameters

{ **-ofnode** {<nodename>|local} } - Node to which Control is Givenback

Specifies the node whose storage is currently taken over by its partner and will be given back by the giveback operation.

| **-fromnode** {<nodename>|local} } - Node Initiating Giveback

Specifies the node that currently holds the storage that is to be returned to the partner node.

[**-require-partner-waiting** {true|false}] - Require Partner in Waiting

If this optional parameter is used and set to false, the storage is given back regardless of whether the partner node is available to take back the storage or not. If this parameter is used and set to true, the storage will not be given back if the partner node is not available to take back the storage. If this parameter is not used, the behavior defaults to the setting of the `-check-partner` option set with the `storage failover modify` command.

[**-override-vetoes** [true]] - Override All Vetoes

If this optional parameter is used, the system overrides veto votes during a giveback operation. If this parameter is not used, the system does not proceed with a giveback if it is vetoed. This parameter, if used, can only be set to true.

[**-only-cfo-aggregates** [true]] - Giveback Only CFO Aggregates

If this optional parameter is used, giveback of only the CFO aggregates (root aggregate and CFO style data aggregates) will be attempted. If this parameter is not used, giveback of all the aggregates (CFO and SFO aggregates) will be attempted. This parameter, if used, can only be set to true.

## Examples

The following example gives back storage that is currently held by a node named `node1`. The partner must be available for the giveback operation to occur.

```
node::> storage failover giveback -fromnode node1 -require-partner-waiting true
```

The following example gives back only the CFO aggregates to a node named `node2` (the aggregates are currently held by a node named `node1`). The partner must be available for the giveback operation to occur, and the veto-giveback process can be overridden.

```
node::> storage failover giveback -ofnode node2 -require-partner-waiting true
```

---

`-override-vetoes true -only-cfo-aggregates true`

## See Also

`storage failover modify` `storage failover show-giveback` `storage aggregate show`

---

## storage failover modify

Modify storage failover attributes

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

### Description

The `storage failover modify` command changes the storage-failover options for a node. Some options are available only at the advanced privilege level and higher.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node whose storage-failover options are to be modified.

{ **[-enabled** {true|false}] - Takeover Enabled

This optionally specifies whether storage failover is enabled. The default setting is `true`.

| **[-mode** {ha|non\_ha}] } - HA Mode

This specifies whether the node is set up in high-availability mode or stand-alone mode. If the node is a member of a high-availability configuration, set the value to `ha`. If the node is stand-alone, set the value to `non_ha`. Before setting the HA mode, you must complete the platform dependent steps to set up the system in a stand-alone or HA configuration as shown in the documentation for your platform.

**[-auto-giveback** {true|false}] - Auto Giveback Enabled

This optionally specifies whether automatic giveback operations are enabled. An automatic giveback operation is invoked when one node of a failover pair is in takeover mode and the failed node is repaired and restarts. When the repaired node boots, the node in takeover mode detects this and initiates a giveback operation. The default setting is `false`, except for two-node clusters where the default setting is `true`.

**[-check-partner** {true|false}] - Check Partner Enabled

This optionally specifies whether the node checks its partner's readiness before initiating a giveback operation when the `storage failover giveback` command is run. The default setting is `true`, which reduces downtime caused by a giveback operation.

**[-detection-time** <integer>] - Takeover Detection Time (secs)

---

This optionally specifies the amount of time, in seconds, that a node remains unresponsive before its partner initiates a takeover operation. Possible values range from 10 to 180 seconds. The default setting is 15 seconds.

**[-onfailure {true|false}]** - Takeover on Failure Enabled (privilege: advanced)

This optionally specifies whether the node automatically takes over for its partner node if the partner node fails. The default setting is `true`. This parameter is available only at the advanced privilege level and higher.

**[-onpanic {true|false}]** - Takeover on Panic Enabled

This optionally specifies whether the node automatically takes over for its partner node if the partner node panics. The default setting is `true`. Changing this parameter on one node automatically makes the same change on its partner node.

**[-onshort-uptime {true|false}]** - Takeover on Short Uptime Enabled (privilege: advanced)

This optionally specifies whether the node takes over for its partner node if the partner node fails within 60 seconds of starting up; the time period is modifiable by using the `-short-uptime` parameter. The default setting is `true`. This parameter is available only at the advanced privilege level and higher.

**[-short-uptime <integer>]** - Short Uptime (secs) (privilege: advanced)

This optionally specifies the time period used by the `-onshort-uptime` parameter. The default setting is 60 seconds. This parameter is available only at the advanced privilege level and higher.

**[-attempts <integer>]** - Number of Giveback Attempts (privilege: advanced)

This optionally specifies the number of times the node attempts an automatic giveback operation within 10 minutes; the time period is modifiable by using the `-attempts-time` parameter. The default setting is 3 attempts. This parameter is available only at the advanced privilege level and higher.

**[-attempts-time <integer>]** - Giveback Attempts Period (minutes) (privilege: advanced)

This optionally specifies the time period used by the `-attempts` parameter. The default setting is 10 minutes. This parameter is available only at the advanced privilege level and higher.

**[-propagate {true|false}]** - Propagate Status via Mailbox (privilege: advanced)

This optionally specifies whether storage-failover status is communicated via mailbox disks. The default setting is `true`. This parameter is available only at the advanced privilege level and higher.

**[-read-interval <integer>]** - Node Status Read Interval (secs) (privilege: advanced)



---

This optionally specifies, in seconds, how frequently the node reads its partner node's status from the mailbox disks. The default setting is 5 seconds. This parameter is available only at the advanced privilege level and higher.

**[-write-interval <integer>]** - Node Status Write Interval (secs) (privilege: advanced)

This optionally specifies, in seconds, how frequently the node writes its status to the mailbox disks. The default setting is 5 seconds. This parameter is available only at the advanced privilege level and higher.

**[-onreboot {true|false}]** - Takeover on Reboot Enabled

This optionally specifies whether the node automatically takes over for its partner if the partner reboots. The default setting is `true`. Takeover can occur if the partner exceeds the expected time to reboot even when this option is set to `false`. The expected time to reboot is different for different platforms. The minimum expected time to reboot is 180 seconds. The `-inhibit-takeover` option of the `system node reboot` command overrides this option: if a node is rebooted with `-inhibit-takeover` set to `true` then takeover does not occur, even if the `takeover on reboot` option is `true`. If a node does takeover due to the partner rebooting, then it will automatically giveback after the reboot, even if the `-auto-giveback` option is set to `false`. This is non-persistent behavior: if the node does takeover due to partner reboot and then itself reboots (prior to giveback) then it will not automatically giveback if the `-auto-giveback` option is set to `false`.

**[-delay-seconds <integer>]** - Delay Before Auto Giveback (secs)

This optionally specifies the minimum time that a node will stay in takeover state prior to performing an automatic giveback. If the taken over node recovers quickly (for example, if the takeover was due to a reboot), by delaying the giveback for a few minutes the outage during the takeover and giveback can be reduced to two short outages instead of one longer one. The allowed range is 0 to 600, inclusive. The default setting is 300 seconds. This option affects all types of auto-giveback. This parameter is available only at the advanced privilege level and higher.

Note:

This delay does not affect manual giveback.

**[-hwassist {true|false}]** - Hardware Assist Enabled

This optionally specifies whether the hardware assist feature is enabled. If set to `true` this feature helps in fast takeover detection times in certain cases.

**[-hwassist-partner-ip <IP Address>]** - Partner's Hwassist IP

---

This optionally specifies the Ip address on which the partner node receives hardware assist alerts. For the hardware assist feature to be active, the value of this option should be equal to partner's node management Ip address.

**[-hwassist-partner-port <integer>]** - Partner's Hwassist Port

This optionally specifies the port number on which partner node listens to hardware assist alerts. It is recommended to have this value to be between 4000-4500. The default value is 4444.

**[-hwassist-health-check-interval <integer>]** - Hwassist Health Check Interval (secs)

This optionally specifies, in seconds, how frequently the hardware assist hardware on a node sends a heartbeat to its partner. The default value is 180.

**[-hwassist-retry-count <integer>]** - Hwassist Retry Count

This optionally specifies the number of times we repeat sending an hardware assist alert. The default value is 2.

**[-auto-giveback-after-panic {true|false}]** - Auto Giveback After Takeover On Panic

This optionally specifies whether a node should attempt automatic giveback operations if takeover was because of a disruption in the partner's operation. An automatic giveback operation is invoked when one node of a failover pair is in takeover mode and the failed node is repaired and restarts. When the repaired node boots, the node in takeover mode detects this and initiates a giveback operation automatically. The default setting is `true`.

**[-bypass-takeover-optimization {true|false}]** - Bypass Takeover Optimization Enabled

This optionally specifies whether operator-initiated planned takeovers will be optimized. If the option is set to `true`, the takeover optimization will be bypassed. If the option is set to `false`, the operator-initiated planned takeover will be optimized. If the planned takeover is optimized, then all SFO aggregates will be relocated serially to the node that is taking over, prior to takeover. This reduces client outage. The default value for this option is `false`.

**[-aggregate-migration-timeout <integer>]** - Aggregate Migration Timeout (secs)  
(privilege: advanced)

This optionally specifies the amount of time, in seconds, the source node has to wait for the destination node to complete the aggregate migration before declaring the migration as failed. The default setting is 120 seconds.

**[-auto-giveback-override-vetoes {true|false}]** - Auto-giveback Override Vetoes Enabled

This optionally specifies whether long-running operations (for instance, NDMP dump/restoration, volume verification, etc.) are terminated and partner veto votes are overridden when an automatic giveback operation is initiated. When this option is set

---

to false, the automatic giveback operation is deferred until the long-running operations have completed and will also take into consideration partner veto votes. The default setting is `false`.

## Examples

The following example enables the storage-failover service on a node named node0:

```
node::> storage failover modify -node node0 -enabled true
```

The following examples enable storage-failover takeover on a short uptime of 30 seconds on a node named node0:

```
node::*> storage failover modify -node node0 -onshort-uptime true -short-uptime  
30
```

## See Also

`storage failover giveback` `system node reboot`

---

## storage failover show-giveback

Display giveback status

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

### Description

The `storage failover show-giveback` command displays information about the giveback status of high-availability (HA) partner aggregates. The command displays the following information when no parameters are specified:

- Node name
- Partner aggregate name
- Giveback Status

You can specify additional parameters to display only the information that matches those parameters. For example, to display information only about a particular aggregate, run the command with the `-aggregate aggregate_name` parameter.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

If this parameter is used, the command displays information about the giveback status of the aggregates belonging to the HA partner of the specified node.

[-aggregate <text>] - Aggregate

If this parameter is used, the command displays information about the giveback status of the specified aggregate.

[-giveback-status <text>, ...] - Aggregates Giveback State

---

If this parameter is used, the command displays information about the aggregates with the specified giveback status.

**[-destination <text>]** - Destination for Giveback

If this parameter is used, the command displays information about the giveback status of the aggregates whose destination after the giveback is the specified node.

### Examples

The following example displays information about giveback status on all nodes:

```
node::> storage failover show-giveback
Node      Partner
Aggregate
-----
node0      -
           No aggregates to give back
node1      -
           No aggregates to give back
node2      -
           No aggregates to give back
node3      -
           No aggregates to give back
4 entries were displayed.
```

---

## storage failover show-takeover

Display takeover status

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

### Description

The `storage failover show-takeover` command displays information about the takeover status of nodes in a cluster. The command also displays the takeover status of aggregates being taken over. During each phase of takeover, the takeover node and the node being taken over display their takeover status and the status of the aggregates being taken over. The command displays the following information when no parameters are specified:

- Node name
- Node takeover status - This contains a descriptive information about the phase of takeover.
- Aggregate
- Aggregate takeover status - This contains the following information:
  - Takeover status of the aggregate, such as "Done", "Failed", "In progress" and "Not attempted yet".
  - Reason for an aggregate takeover failure.
  - Corrective action, in case of an aggregate takeover failure.

You can specify additional parameters to display only the information that matches those parameters. For example, to display information only about a particular node, run the command with the `-node node_name` parameter.

### Parameters

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

If this parameter is specified, the command displays the specified fields for all nodes, in column style output.

| [-instance ] }

If this parameter is specified, the command displays the same detailed information as for the `-node` parameter, but for all nodes.

**`[-node {<nodename>|local}]`** - Node Name

If this parameter is specified, the command displays information about the takeover status of the specified node, and the takeover status of the aggregates being taken over.

**`[-node-takeover-status <text>]`** - Node's Takeover Status

If this parameter is specified, the command displays information about the takeover status of the nodes with the specified node-takeover-status. The command also displays the takeover status of the aggregates belonging to the node being taken over.

**`[-aggregate <text>]`** - Aggregate Being Taken Over

If this parameter is specified, the command displays information about the takeover status of the specified aggregate, and the takeover status of the nodes containing the specified aggregate.

**`[-aggregate-takeover-status <text>]`** - Aggregate's Takeover Status

If this parameter is specified, the command displays information about the takeover status of the aggregates with the specified aggregate takeover status, and the takeover status of the nodes containing those aggregates.

## Examples

The following example shows the takeover status of two nodes, nodeA and nodeB, in an High Availability (HA) pair, when both are in normal mode; neither node has taken over its HA partner. In this case, there is no takeover status for the aggregates.

```
cluster1::> storage failover show-takeover
Node      Node Status      Aggregate      Takeover Status
-----
nodeA     Takeover not
          attempted.
          -
nodeB     Takeover not
          attempted.
          -
```

The following example shows the takeover status of two nodes, nodeA and nodeB, in an HA pair, when nodeA is in the SFO phase of an optimized takeover of nodeB. In this case, nodeA does not have information about the takeover status of nodeB's aggregates.

```
cluster1::> storage failover show-takeover
Node      Node Status      Aggregate      Takeover Status
-----
nodeA     Optimized takeover
          of partner in
          progress. Partner,
          ("nodeB"), is
          relocating its SFO
```

```

aggregates. Run the
command "storage
failover
show-takeover -node
nodeB" to display the
relocation status of
the partner.

nodeB      Being taken over.
backup.

aggr1      In progress, Module:
aggr2      Not attempted yet
CFO aggregates Not attempted yet.

```

The following example shows the takeover status of two nodes, nodeA and nodeB, in an HA pair, when nodeA has completed the SFO phase of an optimized takeover of nodeB (but has not completed the CFO phase of the optimized takeover). In this case, nodeA has information about the takeover status of nodeB's aggregates.

```

cluster1::> storage failover show-takeover
Node      Node Status      Aggregate      Takeover Status
-----
nodeA      Partner has
            relocated its
            aggregates. Takeover
            in progress.
            aggr1      Done
            aggr2      Done
            CFO aggregates In progress.

nodeB      Relocated aggregates
            to partner. Waiting
            for partner to
            takeover.
            aggr1      Done
            aggr2      Done
            CFO aggregates Not attempted
yet.

```

The following example shows the takeover status of two nodes, nodeA and nodeB, in an HA pair, when nodeA has completed the SFO and CFO phases of an optimized takeover of nodeB. In this case, nodeA has information about the takeover status of nodeB's aggregates. Since nodeB is not operational, an Remote Procedure Call(RPC) error is indicated in the command output.

```

cluster1::> storage failover show-takeover
Node      Node Status      Aggregate      Takeover Status
-----
nodeA      Partner has
            relocated its
            aggregates. In
            takeover.
            aggr1      Done
            aggr2      Done
            CFO aggregates Done.
Warning: Unable to list entries on node nodeB. RPC: Port mapper failure - RPC:
Timed out

```

The following example shows the takeover status of two nodes, nodeA and nodeB, in an HA pair, when nodeA has aborted the SFO phase of an optimized takeover of nodeB. In this case, nodeA does not have information about the takeover status of nodeB's aggregates.

```

cluster1::> storage failover show-takeover
Node      Node Status      Aggregate      Takeover Status
-----

```



---

```

-----
nodeA      Optimized takeover
            of partner aborted.
            Run the command
            "storage failover
            show-takeover -node
            nodeB" to display the
            relocation status of
            the partner.

nodeB      Optimized takeover
            by partner aborted.

            Destination node did
            online the aggregate on
            takeover the
            aggregates, run the
            failover takeover
            nodeB
optimization true"
            To giveback the
            aggregates, run the
            failover giveback
            nodeB" command.
            yet
            yet.

            aggr1
            aggr2
            CFO aggregates

            Failed:
            not
            time. To
            remaining
            "storage
            -ofnode
            -bypass-
            command.
            relocated
            "storage
            -ofnode
            Not attempted
            Not attempted

```

---

## storage failover show

Display storage failover status

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

### Description

The `storage failover show` command displays information about storage-failover configurations. By default, the command displays the following information:

- Node name.
- Partner node name.
- Whether storage failover is possible.
- The current state of storage failover. If the takeover is disabled the appropriate reason would be displayed.

To display detailed information about storage failover on a specific node, run the command with the `-node` parameter. The detailed view adds the following information:

- Node NVRAM ID.
- Partner NVRAM ID.
- Whether storage failover is enabled.
- Whether the storage-failover interconnect is available.
- Status of individual storage-failover interconnect links.
- Type and vendor of the storage-failover interconnect.
- Partner State
- Status codes from the takeover-by-partner process. Possible values include:
  - NVRAM\_DOWN
  - OPERATOR\_DISABLE\_NVRAM
  - PARTNER\_RESET
  - FM\_TAKEOVER
  - NVRAM\_MISMATCH

- 
- OPERATOR\_DENY
  - CLUSTER\_DISABLE
  - VERSION
  - SHELF\_HOT
  - REVERT\_IN\_PROGRESS
  - HALT\_NOTKOVER
  - TAKEOVER\_ON\_PANIC
- 
- Reasons why takeover is not possible, if applicable. Possible values include:
    - NOT\_INIT
    - DISABLED
    - DEGRADED
    - MBX\_UNKNOWN
    - FM\_VERSION
    - PARTNER\_DISABLED
    - OPERATOR\_DENY
    - NVRAM\_MISMATCH
    - VERSION
    - IC\_ERROR
    - BOOTING
    - SHELF\_HOT
    - PARTNER\_REVERT\_IN\_PROGRESS
    - LOCAL\_REVERT\_IN\_PROGRESS
    - PARTNER\_TAKEOVER
    - LOCAL\_TAKEOVER
    - HALT\_NOTKOVER
    - LOG\_UNSYNC
    - UNKNOWN
    - WAITING\_FOR\_PARTNER

- 
- LOW\_MEMORY
  - HALTING
  - MBX\_UNCERTAIN
  - NO\_AUTO\_TKOVER
- 
- Time until takeover, in seconds.
  - Time until auto giveback, in seconds.
  - Delay for auto giveback, in seconds.
  - List of local mailbox disks.
  - List of partner mailbox disks.
  - Whether operator-initiated planned takeover will be optimized for performance by relocating SFO (non-root) aggregates serially to the partner prior to takeover.

You can specify additional parameters to select the displayed information. For example, to display information only about storage-failover configurations whose interconnect is down, run the command with `-interconnect-up false`.

## Parameters

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

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

| **[-options ]**

Displays the following information:

- Node name
- Whether automatic giveback operations are enabled
- Whether long-running operations are terminated when an automatic giveback operation is initiated
- Whether the node checks its partner's readiness before initiating a giveback operation
- The time, in seconds, that the node remains unresponsive before its partner initiates a takeover operation
- Whether the node automatically takes over for its partner if the partner fails

- 
- Whether the node automatically takes over for its partner if the partner panics
  - Whether the node automatically takes over for its partner if the partner reboots
  - whether Hardware Assisted Takeover is enabled
  - Ip address on which the partner node listens to the Hardware Assist alerts
  - Port number on which the partner node listens to the Hardware Assist alerts
  - Whether operator-initiated planned takeover will be optimized for performance by relocating SFO (non-root) aggregates serially to the partner prior to takeover

If this parameter is specified when the privilege level is advanced or higher, the display includes the following information:

- Whether the node takes over for its partner if its partner fails after a period of time, which is listed in the following field
- The number of seconds before the node takes over for its partner
- The number of times the node attempts an automatic giveback operation within a period of time
- The number of minutes in which the automatic giveback attempts can occur
- Whether storage-failover status is communicated via mailbox disks
- The interval at which the node reads its partner node's status from the mailbox disks
- The interval at which the node writes its status to the mailbox disks
- The interval at which Hardware assist h/w sends a heartbeat
- The number of times the Hardware assist alert is sent

#### | **[-takeover-status]**

Displays the following information:

- Node name
- Partner name
- Takeover enabled
- Takeover possible
- Interconnect up
- State

- 
- Node NVRAM ID
  - Partner NVRAM ID
  - Reason Takeover Not Possible By Partner
  - Reason Takeover Not Possible
  - Time Until Takeover

| **[-advanced]** (privilege: advanced)

Displays the following information:

- Node name
- Whether kill messages are issued during a takeover operation
- Whether the node controls its partner's storage aggregates
- The time when firmware notification was received
- The time when booting notification was received
- The time at which the last takeover or giveback operation occurred, in microseconds
- The number of times the failover log was unsynchronized

| **[-iotime]** (privilege: advanced)

Displays the following information:

- Node name
- Primary normal I/O time
- Primary transition I/O time
- Backup normal I/O time
- Backup transition I/O time

| **[-mailbox-status]** (privilege: advanced)

Displays the following information:

- Node name
- Primary mailbox status
- Backup mailbox status

---

| **[-more-options]** (privilege: advanced)

Displays the following information:

- Node name
- Whether takeover on short uptime is enabled
- Short uptime, in seconds
- Number of giveback attempts
- Interval of giveback attempts, in minutes
- Whether the primary mailbox is online
- Mailbox status read interval, in seconds
- Mailbox status write interval, in seconds

| **[-progress]** (privilege: advanced)

Displays the following information:

- Node name
- Maximum resource-table index number
- Current resource-table index number
- Current resource-table entry

| **[-timeout]** (privilege: advanced)

Displays the following information:

- Node name
- Fast timeout
- Slow timeout
- Mailbox timeout
- Connection timeout
- Operator timeout
- Firmware timeout
- Dump-core timeout
- Booting timeout

- 
- Reboot timeout

| **[-transit ]** (privilege: advanced)

Displays the following information:

- Node name
- Transit Timer Enabled
- Transit Timeout

| **[-instance ]** }

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

**[-node {<nodename>|local}]** - Node

Selects the nodes whose name matches this parameter value.

**[-partner-name <text>]** - Partner Name

Selects the nodes that have the specified partner-name setting.

**[-nvramid <integer>]** - Node NVRAM ID

Selects the nodes that have the specified NVRAM ID setting.

**[-partner-nvramid <integer>]** - Partner NVRAM ID

Selects the nodes that have the specified partner NVRAM ID setting.

**[-enabled {true|false}]** - Takeover Enabled

Selects the nodes that have the specified takeover-enablement setting.

**[-mode {ha|non\_ha}]** - HA Mode

Selects the nodes that have the specified HA-mode setting. If the value is `ha` then the node is a member of a storage-failover configuration. If it is `non-ha` then it is in a stand-alone configuration.

**[-possible {true|false}]** - Takeover Possible

Selects the nodes that have the specified failover-possible setting.

**[-reason <text>, ...]** - Reason Takeover not Possible

Selects the nodes that have the specified reason-not-possible setting. Possible values include:

- NOT\_INIT



- 
- DISABLED
  - DEGRADED
  - MBX\_UNKNOWN
  - FM\_VERSION
  - PARTNER\_DISABLED
  - OPERATOR\_DENY
  - NVRAM\_MISMATCH
  - VERSION
  - IC\_ERROR
  - BOOTING
  - SHELF\_HOT
  - PARTNER\_REVERT\_IN\_PROGRESS
  - LOCAL\_REVERT\_IN\_PROGRESS
  - PARTNER\_TAKEOVER
  - LOCAL\_TAKEOVER
  - HALT\_NOTKOVER
  - LOG\_UNSYNC
  - UNKNOWN
  - WAITING\_FOR\_PARTNER
  - LOW\_MEMORY
  - HALTING
  - MBX\_UNCERTAIN
  - NO\_AUTO\_TKOVER

**[-interconnect-up {true|false}]** - Interconnect Up

Selects the nodes that have the specified interconnect-up setting.

**[-interconnect-links <text>]** - Interconnect Links

Selects the nodes that have the specified interconnect-links setting.

**[-interconnect-type <text>]** - Interconnect Type

---

Selects the nodes that have the specified interconnect-type setting.

**[-state-description <text>]** - State Description

Selects the nodes that have the specified state-description setting.

**[-partner-state <text>]** - Partner State

Selects the nodes that have the specified partner-state setting. Possible values include:

- OPERATOR COMPLETED
- DEBUGGUER COMPLETED
- PROGRESS COUNTER
- I/O ERROR
- BAD CHECKSUM
- RESERVED
- UNKNOWN
- INITIALIZING
- IN POWER-ON SELF TEST
- BOOTING
- BOOT FAILED
- WAITING
- KERNEL LOADED
- UP
- IN DEBUGGER
- WAITING FOR OPERATOR INPUT
- DUMPING CORE
- HALTED
- REBOOTING
- WAITING FOR GIVEBACK (DISK RESERVATIONS)
- WAITING FOR GIVEBACK (HA MAILBOXES)
- DUMPING SPARECORE
- MULTI-DISK PANIC

- 
- IN TAKEOVER

**[-time-until-takeover <integer>]** - Time Until Takeover

Selects the nodes that have the specified time-until-takeover setting.

**[-partner-reason <text>, ...]** - Reason Takeover not Possible by Partner

Selects the nodes that have the specified partner-reason text setting.

**[-killpackets {true|false}]** - Issue Kill Packets (privilege: advanced)

Selects the nodes that have the specified kill packets setting.

**[-partner-aggregates {true|false}]** - Control Partner Aggregates (privilege: advanced)

Selects the nodes that have the specified partner aggregates setting.

**[-current-index <integer>]** - Current Progress Index (privilege: advanced)

Selects the nodes that have the specified current-progress index setting.

**[-current-entry <text>]** - Current Progress Entry (privilege: advanced)

Selects the nodes that have the specified current-progress entry setting.

**[-maximum-index <integer>]** - Maximum Progress Index (privilege: advanced)

Selects the nodes that have the specified maximum-progress index setting.

**[-pmbox-status <text>, ...]** - Primary Mailbox Status (privilege: advanced)

Selects the nodes that have the specified primary mailbox status setting. Possible values include:

- MBX\_STATUS\_NODISKS
- MBX\_STATUS\_UNCERTAIN
- MBX\_STATUS\_STALE
- MBX\_STATUS\_CONFLICTED
- MBX\_STATUS\_OLD\_VERSION
- MBX\_STATUS\_NOT\_FOUND
- MBX\_STATUS\_WRONG\_STATE
- MBX\_STATUS\_BACKUP

**[-bmbox-status <text>, ...]** - Backup Mailbox Status (privilege: advanced)

---

Selects the nodes that have the specified backup-mailbox status setting. See the description of the `-pmbox-status` parameter for a list of possible values.

**[-local-mbx-node-status <Mailbox Status>]** - Local Mailbox Node Status (privilege: advanced)

Selects the nodes that have the specified local mailbox node status. Possible values include:

- `MBX_UNKNOWN` - Local node is up, mailbox uninitialized
- `MBX_TAKEOVER_DISABLED` - Local node is up but takeover is disallowed
- `MBX_TAKEOVER_ENABLED` - Local node is up and takeover is allowed
- `MBX_TAKEOVER_ACTIVE` - Partner node has taken over
- `MBX_GIVEBACK_DONE` - Giveback completed, but local node has not yet restarted

**[-partner-mbx-node-status <Mailbox Status>]** - Partner Mailbox Node Status (privilege: advanced)

Selects the nodes that have the specified partner mailbox node status. Possible values include:

- `MBX_UNKNOWN`
- `MBX_TAKEOVER_DISABLED`
- `MBX_TAKEOVER_ENABLED`
- `MBX_TAKEOVER_ACTIVE`
- `MBX_GIVEBACK_DONE`

**[-local-takeover-info <text>]** - Local Takeover Info (privilege: advanced)

Selects the nodes that have the specified local node takeover information. This includes the type of negotiated failover request, or if takeover is not possible, the reason why takeover is disabled. Possible values include:

- `NOTKOVER_NVRAM_DOWN` - NVRAM mirror is down
- `NOTKOVER_OPERATOR_DISABLE_NVRAM` - Operator disabled
- `NOTKOVER_PARTNER_RESET` - A link reset is in progress
- `NOTKOVER_FM_TAKEOVER` - The failover monitor has declared takeover
- `NOTKOVER_NVRAM_MISMATCH` - NVRAM sizes mismatch

- 
- NOTKOVER\_OPERATOR\_DENY - Operator denies takeover
  - NOTKOVER\_CLUSTER\_DISABLE - Cluster is disabled
  - NOTKOVER\_VERSION - Version mismatch
  - NOTKOVER\_SHELF\_HOT - Disk shelf is too hot
  - NOTKOVER\_REVERT\_IN\_PROGRESS - Revert is in progress
  - NOTKOVER\_HALT\_NOTKOVER - Node halted in no-takeover mode
  - TKOVER\_ON\_REBOOT - Enable takeover on reboot
  - TKOVER\_ON\_PANIC - Enabled takeover on panic
  - TKOVER\_ON\_STUTTER\_DISABLED - Disable takeover on short uptime
  - NFO\_DISK\_SHELF\_ENABLED - Negotiated failover for disk shelf module is enabled
  - NFO\_NWK\_IF\_ENABLED - Negotiated failover for network module is enabled
  - NFO\_ISCSI\_ENABLED - Negotiated failover for network interfaces module is enabled
  - NFO\_FCP\_TARGET\_ENABLED - Negotiated failover for fcp target module is enabled

**[-partner-takeover-info <text>]** - Partner Takeover Info (privilege: advanced)

Selects the nodes that have the specified partner node takeover information. This includes the type of negotiated failover request, or if takeover is not possible, the reason why takeover is disabled. Possible values include:

- NOTKOVER\_NVRAM\_DOWN - NVRAM mirror is down
- NOTKOVER\_OPERATOR\_DISABLE\_NVRAM - Operator disabled
- NOTKOVER\_PARTNER\_RESET - A link reset is in progress
- NOTKOVER\_FM\_TAKEOVER - The failover monitor has declared takeover
- NOTKOVER\_NVRAM\_MISMATCH - NVRAM sizes mismatch
- NOTKOVER\_OPERATOR\_DENY - Operator denies takeover
- NOTKOVER\_CLUSTER\_DISABLE - Cluster is disabled
- NOTKOVER\_VERSION - Version mismatch
- NOTKOVER\_SHELF\_HOT - Disk shelf is too hot
- NOTKOVER\_REVERT\_IN\_PROGRESS - Revert is in progress

- 
- NOTKOVER\_HALT\_NOTKOVER - Node halted in no-takeover mode
  - TKOVER\_ON\_REBOOT - Takeover on reboot is enabled
  - TKOVER\_ON\_PANIC - Takeover on panic is enabled
  - TKOVER\_ON\_STUTTER\_DISABLED - Disable takeover on short uptime
  - NFO\_DISK\_SHELF\_ENABLED - Negotiated failover for disk shelf module is enabled
  - NFO\_NWK\_IF\_ENABLED - Negotiated failover for network module is enabled
  - NFO\_ISCSI\_ENABLED - Negotiated failover for network interfaces module is enabled
  - NFO\_FCP\_TARGET\_ENABLED - Negotiated failover for fcp target module is enabled

**[-local-headswap-state <Headswap State>]** - Local Head Swap State (privilege: advanced)

Selects the nodes that have the specified local node headswap state. Possible values are:

- HEADSWAP\_NONE - head swap not in progress
- HEADSWAP\_START - head swap started
- HEADSWAP\_CFO\_START - CFO phase of head swap started
- HEADSWAP\_CFO\_END - CFO phase of head swap completed
- HEADSWAP\_SFO\_START - SFO phase of head swap started

**[-partner-headswap-state <Headswap State>]** - Partner Head Swap State (privilege: advanced)

Selects the nodes that have the specified partner node headswap state. Possible values are:

- HEADSWAP\_NONE - head swap not in progress
- HEADSWAP\_START - head swap started
- HEADSWAP\_CFO\_START - CFO phase of head swap started
- HEADSWAP\_CFO\_END - CFO phase of head swap completed
- HEADSWAP\_SFO\_START - SFO phase of head swap started

**[-fast-timeout <integer>]** - Fast Timeout (privilege: advanced)

---

Selects the nodes that have the specified fast-timeout configuration setting.

**[-slow-timeout <integer>]** - Slow Timeout (privilege: advanced)

Selects the nodes that have the specified slow-timeout setting.

**[-mailbox-timeout <integer>]** - Mailbox Timeout (privilege: advanced)

Selects the nodes that have the specified mailbox-timeout setting.

**[-connect-timeout <integer>]** - Connect Timeout (privilege: advanced)

Selects the nodes that have the specified connect-timeout setting.

**[-operator-timeout <integer>]** - Operator Timeout (privilege: advanced)

Selects the nodes that have the specified operator-timeout setting.

**[-firmware-timeout <integer>]** - Firmware Timeout (privilege: advanced)

Selects the nodes that have the specified firmware-timeout setting.

**[-dumpcore-timeout <integer>]** - Dumpcore Timeout (privilege: advanced)

Selects the nodes that have the specified dump-core timeout setting.

**[-booting-timeout <integer>]** - Booting Timeout (privilege: advanced)

Selects the nodes that have the specified booting-timeout setting.

**[-transit-timer {true|false}]** - Transit Timer Enabled (privilege: advanced)

Selects the nodes that have the specified transit-timer setting.

**[-transit-timeout <integer>]** - Transit Timeout (privilege: advanced)

Selects the nodes that have the specified transit timeout.

**[-firmware-received <integer>]** - Firmware Received (privilege: advanced)

Selects the nodes that have the specified firmware-reception time.

**[-firmware-received-cycles <integer>]** - Firmware Received in CPU Cycles (privilege: advanced)

Selects the nodes that have the specified firmware-reception time in CPU Cycles.

**[-booting-received <integer>]** - Booting Received (privilege: advanced)

Selects the nodes that have the specified booting-reception time.

**[-transit-time <integer>]** - Transit Event Time (privilege: advanced)

Selects the nodes whose last failover event occurred at the specified time.

**[-pnormal <integer>]** - Primary Normal IO Time (privilege: advanced)

---

Selects the nodes that have the specified normal primary-mailbox I/O time.

**[-ptransition <integer>]** - Primary Transition IO Time (privilege: advanced)

Selects the nodes that have the specified transitional primary-mailbox I/O time.

**[-bnormal <integer>]** - Backup Normal IO Time (privilege: advanced)

Selects the nodes that have the specified normal backup-mailbox I/O time.

**[-btransition <integer>]** - Backup Transition IO Time (privilege: advanced)

Selects the nodes that have the specified transitional backup-mailbox I/O time.

**[-logs-unsynced <integer>]** - Logs Unsynced Count (privilege: advanced)

Selects the nodes that have the specified count of unsynchronized logs.

**[-auto-giveback {true|false}]** - Auto Giveback Enabled

Selects the nodes that have the specified auto-giveback setting.

**[-check-partner {true|false}]** - Check Partner Enabled

Selects the nodes that have the specified partner-checking setting.

**[-detection-time <integer>]** - Takeover Detection Time (secs)

Selects the nodes that have the specified detection-time setting.

**[-onfailure {true|false}]** - Takeover on Failure Enabled (privilege: advanced)

Selects the nodes that have the specified takeover-on-failure setting.

**[-onpanic {true|false}]** - Takeover on Panic Enabled

Selects the nodes that have the specified takeover-on-panic setting.

**[-onshort-uptime {true|false}]** - Takeover on Short Uptime Enabled (privilege: advanced)

Selects the storage-failover configurations that match this parameter value.

**[-short-uptime <integer>]** - Short Uptime (secs) (privilege: advanced)

Selects the nodes that have the specified short-uptime value.

**[-attempts <integer>]** - Number of Giveback Attempts (privilege: advanced)

Selects the nodes that have the specified number of giveback attempts.

**[-attempts-time <integer>]** - Giveback Attempts Period (minutes) (privilege: advanced)

Selects the nodes that have the specified time setting for giveback attempts.

**[-propagate {true|false}]** - Propagate Status via Mailbox (privilege: advanced)



---

Selects the nodes that have the specified propagate-status-via-mailbox setting.

**[-read-interval <integer>]** - Node Status Read Interval (secs) (privilege: advanced)

Selects the nodes that have the specified read interval.

**[-write-interval <integer>]** - Node Status Write Interval (secs) (privilege: advanced)

Selects the nodes that have the specified write interval.

**[-onreboot {true|false}]** - Takeover on Reboot Enabled

Selects the nodes that have the specified takeover-on-reboot setting.

**[-delay-seconds <integer>]** - Delay Before Auto Giveback (secs)

Selects the nodes that have the specified delay (in seconds) for the auto giveback.

**[-hwassist {true|false}]** - Hardware Assist Enabled

Selects the nodes that have the specified hwassist setting.

**[-hwassist-partner-ip <IP Address>]** - Partner's Hwassist IP

Selects the nodes that have the specified hwassist-partner-ip setting.

**[-hwassist-partner-port <integer>]** - Partner's Hwassist Port

Selects the nodes that have the specified hwassist-partner-port setting.

**[-hwassist-health-check-interval <integer>]** - Hwassist Health Check Interval (secs)

Selects the nodes that have the specified hwassist health check interval, in seconds.

**[-hwassist-retry-count <integer>]** - Hwassist Retry Count

Selects the nodes that have the specified hwassist retry count, in seconds.

**[-hwassist-status <text>]** - Hwassist Status

Selects the nodes that have the specified hwassist-status setting.

**[-time-until-autogiveback <integer>]** - Time Until Auto Giveback (secs)

Selects the nodes that have the specified time(in seconds) until auto giveback.

**[-local-mailbox-disks <text>]** - Local Mailbox Disks

Selects the nodes that have the specified mailbox disks on the local node.

**[-partner-mailbox-disks <text>]** - Partner Mailbox Disks

Selects the nodes that have the specified mailbox disks on the partner node.

**[-local-firmware-state <text>]** - Local Firmware State (privilege: advanced)

---

Selects the nodes that have the specified firmware state on the local node.

**[-local-firmware-progress <integer>]** - Local Firmware Progress Counter (privilege: advanced)

Selects the nodes that have the specified firmware progress counter for the local node.

**[-partner-firmware-state <text>]** - Partner Firmware State (privilege: advanced)

Selects the nodes that have the specified firmware state of the partner node.

**[-partner-firmware-progress <integer>]** - Partner Firmware Progress Counter (privilege: advanced)

Selects the nodes that have the specified firmware progress counter for the partner node.

**[-local-missing-disks <text>]** - Missing Disks on Local Node

Selects the nodes that have the specified missing disks on the local node.

**[-partner-missing-disks <text>]** - Missing Disks on Partner Node

Selects the nodes that have the specified missing disks on the partner node.

**[-reboot-timeout <integer>]** - Reboot Timeout (privilege: advanced)

Selects the nodes that have the specified reboot timeout.

**[-time-since-takeover <text>]** - Time Since Takeover

Selects the nodes that have been in takeover mode for the specified amount of time.

**[-auto-giveback-after-panic {true|false}]** - Auto Giveback After Takeover On Panic

Selects the nodes that have the specified auto-giveback-after-panic setting. If true then an automatic giveback operation is invoked when the failover node of an HA pair is repaired and rebooted. The takeover node of the HA pair detects this and initiates a giveback operation automatically.

**[-is-giveback-requested {true|false}]** - Giveback Requested (privilege: advanced)

Selects the nodes that have the specified is-giveback-requested setting. If true, a deferred giveback request has been made by the local node.

**[-auto-giveback-last-veto-check <integer>]** - Auto Giveback Last Veto Check (privilege: advanced)

Selects the nodes that have the specified auto-giveback-last-veto-check time. This setting indicates the time, in milliseconds, when the local node made the most recent giveback veto check.

---

**[-is-auto-giveback-attempts-exceeded {true|false}]** - Auto Giveback Attempts Exceeded (privilege: advanced)

Selects the nodes that have the specified is-auto-giveback-attempts-exceeded setting. If true, the local node has exceeded the maximum number of allowed auto giveback attempts.

**[-was-auto-giveback-done {true|false}]** - Was Auto Giveback Done (privilege: advanced)

Selects the nodes that have the specified was-auto-giveback-done setting. If true, the last giveback was automatic (as opposed to a manual giveback).

**[-is-cifs-auto-giveback-stopping {true|false}]** - Is CIFS Auto Giveback Stopping (privilege: advanced)

Selects the nodes that have the specified is-cifs-auto-giveback-stopping setting. If true, the local node has initiated CIFS termination as part of an automatic giveback.

**[-bypass-takeover-optimization {true|false}]** - Bypass Takeover Optimization Enabled

Selects the nodes that have the specified bypass-takeover-optimization setting. If the value is true then optimized operator-initiated planned takeover is bypassed. Operator initiated planned takeover is optimized when SFO aggregates are relocated serially to the partner prior to takeover. This reduces client outage. If the value is false then optimized operator-initiated planned takeover is enabled on this node.

**[-aggregate-migration-timeout <integer>]** - Aggregate Migration Timeout (secs) (privilege: advanced)

Selects the nodes that have the specified aggregate migration timeout.

**[-auto-giveback-override-vetoes {true|false}]** - Auto-giveback Override Vetoes Enabled

Selects the nodes that have the specified auto-giveback-override-vetoes setting.

**[-is-mirror-enabled {true|false}]** - Is NVRAM Mirroring Enabled (privilege: advanced)

Selects the nodes that have the specified is-mirror-enabled setting. If true, then NVRAM mirroring is enabled.

**[-is-mirror-consistency-required {true|false}]** - Is Mirror Consistency Required (privilege: advanced)

Selects the nodes that have the specified is-mirror-consistency-required setting. If true, then NVRAM mirror consistency is required.

**[-is-degraded {true|false}]** - Are Partner Mailbox Disks Not Known (privilege: advanced)

Selects the nodes that have the specified is-degraded setting. If true, takeovers are deferred because partner mailbox disks are not known.

---

**[-reserve-policy <reserve policy>]** - FM Reservation Policy (privilege: advanced)

Selects the nodes that have the specified disk reservation policy. Possible values are:

- **RESERVE\_NO\_DISKS** - no disk reservations made during takeover, nor are disk reservations released during giveback
- **RESERVE\_LOCK\_DISKS\_ONLY** - only mailbox disks are released during takeover and released during giveback
- **RESERVE\_ONLY\_AT\_TAKEOVER** - reservations are issued only at takeover time. All disks are reserved. All reservations are released at giveback
- **RESERVE\_ALWAYS\_AFTER\_TAKEOVER** - reservations are issued at at takeover. When disks are subsequently added, they are also reserved. All disks are released at giveback

**[-total-system-uptime <integer>]** - Total System Uptime (privilege: advanced)

Selects the nodes that have the specified total system uptime, in milliseconds.

**[-current-time <integer>]** - Current System Time (privilege: advanced)

Selects the nodes that have the specified current time on the filer.

**[-fm-takeover-state <FM Takeover/Giveback Transition>]** - FM Takeover State (privilege: advanced)

Selects the nodes that have the specified takeover state. Possible values are:

- **FT\_NONE** - Not in takeover
- **FT\_TAKEOVER\_STARTED** - Local node has initiated takeover
- **FT\_TAKEOVER\_COMMITTED** - Takeover has been committed
- **FT\_TAKEOVER\_DONE\_OK** - Local node successfully completed takeover
- **FT\_TAKEOVER\_DONE\_FAILED** - Takeover failed

**[-fm-giveback-state <FM Takeover/Giveback Transition>]** - FM Giveback State (privilege: advanced)

Selects the nodes that have the specified giveback state. Possible values are:

- **FT\_NONE** - Not in giveback
- **FT\_GIVEBACK\_READY** - Partner node is ready for giveback
- **FT\_GIVEBACK\_STARTED** - Local node has initiated giveback
- **FT\_GIVEBACK\_COMMITTED** - Giveback has been committed

- 
- FT\_GIVEBACK\_DONE\_OK - Giveback completed successfully

## Examples

The following example displays information about all storage-failover configurations:

```
cluster1::> storage failover show
Node      Partner  Takeover Possible State
-----
node0     node1    true      Connected to node1
node2     node3    true      Connected to node3
node1     node0    true      Connected to node0
node3     node2    true      Connected to node2
4 entries were displayed.
```

---

## storage failover takeover

Take over the storage of a node's partner

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

### Description

The `storage failover takeover` command initiates a takeover of the partner node's storage.

### Parameters

{ **-ofnode** {<nodename>|local} } - Node to Takeover

This specifies the node that is taken over. It is shut down and its partner takes over its storage.

| **-bynode** {<nodename>|local} } - Node Initiating Takeover

This specifies the node that is to take over its partner's storage.

[**-option** <takeover option>] - Takeover Option

This optionally specifies the style of takeover operation. Possible values include the following:

- **normal** - Specifies a normal takeover operation; that is, the partner is given the time to close its storage resources gracefully before the takeover operation proceeds. This is the default value.
- **immediate** - Specifies an immediate takeover. In an immediate takeover, the takeover operation is initiated before the partner is given the time to close its storage resources gracefully. The use of this option results in an immediate takeover which does not do a clean shutdown. In case of NDU this can result in a NDU failure.

Attention:

If this option is specified, negotiated takeover optimization is bypassed even if the `-bypass-optimization` option is set to false.

- **allow-version-mismatch** - If this value is specified, the takeover operation is initiated even if the partner is running a version of software that is incompatible

---

with the version running on the node. In this case, the partner is given the time to close its storage resources gracefully before the takeover operation proceeds. Use this value as part of a nondisruptive upgrade procedure.

- **force** - If this value is specified, the takeover operation is initiated even if the node detects an error that normally prevents a takeover operation from occurring. This value is available only at the advanced privilege level and higher.

Attention:

If this option is specified, negotiated takeover optimization is bypassed even if the `-bypass-optimization` option is set to false.

Caution:

The use of this option can potentially result in data loss. If the HA interconnect is detached or inactive, or the contents of the failover partner's NVRAM cards are unsynchronized, takeover is normally disabled. Using the `-force` option enables a node to take over its partner's storage despite the unsynchronized NVRAM, which can contain client data that can be lost upon storage takeover.

#### **`[-bypass-optimization {true|false}]` - Bypass Takeover Optimization**

If this is an operator-initiated planned takeover, this parameter specifies whether the takeover optimization is bypassed. This parameter defaults to false.

Attention:

This parameter is ignored and negotiated takeover optimization automatically bypassed if the `-immediate` option, the `-force` option, or the `-allow-disk-inventory-mismatch` parameter is specified as part of the same storage failover takeover command.

#### **`[-allow-disk-inventory-mismatch {true|false}]` - Disk inventory**

If this parameter is specified, the takeover operation is initiated even if the local node cannot see the partner's filesystem disks.

Attention:

If this parameter is specified, negotiated takeover optimization is bypassed even if the `-bypass-optimization` parameter is set to false.

Caution:

---

The use of this parameter can potentially result in client outage.

### **`[-skip-lif-migration [true]]` - Skip LIF Migration**

This parameter specifies that LIF migration prior to takeover is skipped. Without this parameter, the command attempts to synchronously migrate data and cluster management LIFs away from the node prior to its takeover. If the migration fails or times out, the takeover is aborted.

## **Examples**

The following example causes a node named node0 to initiate a negotiated optimized takeover of its partner's storage:

```
cluster1::> storage failover takeover -bynode node0
```

The following example causes a node named node0 to initiate an immediate takeover of its partner's storage:

```
cluster1::> storage failover takeover -bynode node0 -option immediate
```

## **storage failover hwassist show**

Display hwassist status

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

## **Description**

The `storage failover hwassist show` command displays information about hardware assisted takeover configurations. By default, the command displays the following information:

- Node name.
- Partner node name.
- Whether hardware assisted takeover is enabled.
- IP address on which the local node receives hardware assist alerts.
- Port on which local node receives hardware assist alerts.
- Hardware assist monitor status.
- If the monitor is inactive, the reason it is inactive.
- If the monitor is inactive, the corrective action to make it active.



---

## Parameters

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

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

| [-instance ] }

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

**[-node {<nodename>|local}]** - Node

Selects the hwassist configurations that match this parameter value.

**[-partner-name {<nodename>|local}]** - Name of the Partner Node

Selects the hwassist configurations that match this parameter value.

**[-enabled {true|false}]** - Local Hardware Assist Enabled

Selects the hwassist configurations that match this parameter value.

**[-local-status <text>]** - Local Node's Hwassist Status

Selects the hwassist configurations that match this parameter value (active or inactive).

**[-local-ip <text>]** - IP Address on Which Local Node is Listening

Selects the hwassist configurations that match this parameter value.

**[-local-port <integer>]** - Port on Which Local Node is Listening

Selects the hwassist configurations that match this parameter value.

**[-local-inactive <text>]** - Local Node's Hwassist Inactive Status Reason

Selects the hwassist configurations that match this parameter value.

**[-local-action <text>]** - Corrective Action on Local Node

Selects the hwassist configurations that match this parameter value.

## Examples

The following example displays the hardware assist information for the local node and its partner:

```
cluster1::> storage failover hwassist show
Node
-----
ha1
Partner : ha2
```

---

ha2

    Hwassist Enabled : true  
        Hwassist IP : 10.225.248.19  
        Hwassist Port : 4444  
        Monitor Status : active  
        Inactive Reason : -  
Corrective Action : -

        Partner : hal  
    Hwassist Enabled : true  
        Hwassist IP : 10.225.248.21  
        Hwassist Port : 4444  
        Monitor Status : active  
        Inactive Reason : -  
Corrective Action : -

---

## storage failover hwassist test

Test the hwassist functionality

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

### Description

The `storage failover hwassist test` command tests the Hardware Assist h/w connectivity between the two nodes in a HA pair. The test result can be one of the following.

- Hardware Assist is not initialized.
- No Hardware Assist h/w found.
- Partner is throttling alerts.
- Resource is busy.
- Hardware Assist h/w returned an error.
- No response from partner.Timed out.
- Unexpected abort.
- Partner has taken over.
- Interconnect is down between nodes.
- Partner is not booted up yet.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node from which a test alert is initiated.

### Examples

The following command issues a test alert from the node ha1:

```
ha1::> storage failover hwassist test -node ha1
Info: Storage Failover Hwassist: Operation successful.
```

---

## storage failover hwassist stats clear

Clear the hwassist statistics

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

### Description

The `storage failover hwassist stats clear` command clears the statistics information maintained by Hardware Assist functionality.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the statistics are to be cleared.

### Examples

The following example clears the hwassist statistics on the node ha1:

```
ha1:: > storage failover hwassist stats clear -node ha1
```

## storage failover hwassist stats show

Display hwassist statistics

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

### Description

The `storage failover hwassist stats show` command displays statistics about the hardware assist alerts processed by a node. The command displays the following information for each alert:

- Alert type.
- Event that triggered the alert.
- The number of times the alert has been received.
- Whether takeover was possible on receiving the alert.

- The last time at which the alert was received.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Selects the hwassist statistics for the specified node.

### Examples

The following example displays the hwassist statistics for the node ha1:

```
cluster1::> storage failover hwassist stats show -node ha1
Node
recieved
-----
ha1
system_down power_loss 0 Yes ---
system_down l2_watchdog_reset 0 Yes ---
system_down power_off_via_rlm 0 Yes ---
system_down power_cycle_via_rlm 0 Yes ---
system_down reset_via_rlm 0 Yes ---
system_down power_off_via_sp 0 Yes ---
system_down power_cycle_via_sp 0 Yes ---
system_down reset_via_sp 0 Yes ---
system_down post_error 0 No ---
system_down abnormal_reboot 0 No ---
system_down loss_of_heartbeat 0 No ---
keep_alive periodic_message 121 No Thu Feb
10 13:10:52 EST 2011
test test 0 No ---
ID mismatch --- 0 --- ---
Key mismatch --- 0 --- ---
Unknown --- 0 --- ---
Number of times hw_assist alerts throttled: 0
```

---

## storage failover interconnect show-link

Display information about the storage failover interconnect link

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

### Description

The `storage failover interconnect show-link` command displays information about storage failover interconnect links in the cluster.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Use this parameter to display information only about the interconnect links on the specified node.

[-link-number <integer>] - Link Number

Use this parameter to display information only about nodes that have the number of interconnect links you specify.

[-link-state <text>] - Link State

Use this parameter to display information only about the interconnect links that are in the state you specify. Possible values include `up` and `down`.

### Examples

The following example displays information about all storage-failover interconnect links in the cluster:

```
cluster1::*> storage failover interconnect show-link
Node      Port Number      Link State
-----
node1
```

---

	0	down
	1	up
node2	0	down
	1	up

4 entries were displayed.

---

## storage failover interconnect status

Display the state of the storage failover interconnect and active logical links

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

### Description

The `storage failover interconnect status` command displays status information about storage failover interconnects in the cluster.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Use this parameter to display information only about the interconnect status of the nodes you specify.

[-state <text>] - Storage Failover Connection State

Use this parameter to display information only about the interconnects that are in the state you specify. Possible values are `connected` and `disconnected`.

[-active-link <integer>] - Active Logical Link

Use this parameter to display information only about the interconnects that have the number of active logical links that you specify.

### Examples

The following example displays storage-failover interconnect status for all nodes in the cluster:

```
cluster1::*> storage failover interconnect status
Node           Connection State      Active Logical Link
-----
node1
```



---

node2	Disconnected	1
2 entries were	Disconnected	1
displayed.		

---

## storage failover interconnect statistics error show

Display error statistics for the storage failover interconnect

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

### Description

The `storage failover interconnect statistics error show` command displays node-specific error statistics about the storage-failover interconnect.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects error statistics for the specified node.

[-**type** {rv|nvram5-sw|nvram5-hw-error|nvram5-hw-perf|nvram5-port-1|nvram5-port-2}] - Error Statistics Type

Selects the error statistics of the specified type.

[-**counter** <text>] - Error Counter Name

Selects the error statistics for the specified error counter.

[-**value** <integer>] - Error Counter Value

Selects the error statistics that match the specified counter value.

### Examples

The following example displays the counter named `RV connection attempts` for statistic type `RV` on the node named `node0`:

```
cluster1::*> storage failover interconnect statistics error show -node node0 -
type RV -counter "RV connection attempts"
Node Name : node0
```

---

Error Statistics Type : RV  
Error Counter Name : RV connection attempts  
Counter Value : 2

---

# storage failover interconnect statistics performance basic

Display basic performance statistics for the storage failover interconnect

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

## Description

The `storage failover interconnect statistics performance basic` command displays basic performance statistics for the storage-failover interconnect.

## Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Specify this parameter to display only statistics for the node you specify.

[-**counter** <text>] - Error Counter Name

Specify this parameter to display only the statistic counter you specify.

[-**value** <integer>] - Error Counter Value

Specify this parameter to display only statistics that have the value you specify.

## Examples

The following example displays basic performance statistics for a node named `node0`:

```
cluster1::*> storage failover interconnect statistics performance basic -node
node0
Node      Counter Name                                     Counter Value
-----
node0
      Avg MB/s                                         8
      Completion Intr rate(per sec)                  0
      Elapsed time(secs)                             2913
      RDMA reads                                       2914
```

---

avg bytes per xfer	6281
avg ic_waitdone RDMA-READ time(us)	0
avg ic_waitdone time(us)	49
avg nv_vl_q lengths	0
avg rnv transfer size	8408
avg time between rnv msgs(us)	2113
avg time between rnv transfers(us)	1056
ic_16K+_writes	606052
ic_4k_writes	621335
ic_8k_writes	475766
ic_isdone	2489583
ic_isdone done	411252
ic_isdone not-done	2078331
ic_qmax_waits	0
ic_small_writes:	2388998
ic_waits	1006419
nvlog Avg time to sync(msec)	530
nvlog Max time to sync(msec)	530
rnv msgs dequeued	1378876
rnv msgs not queued	82
rnv msgs queued	1378876
rnv queue total waittime(us)	72775524
rnv transfers	2757936
total xfers	4092323

28 entries were displayed.

---

## storage failover interconnect statistics performance vi-if

Display vi-if performance statistics for the storage failover interconnect

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

### Description

The `storage failover interconnect statistics performance vi-if` command displays performance statistics on a per-interface basis for the storage-failover interconnect.

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Specify this parameter to display only statistics for the node you specify.

[-**interface** <integer>] - VI\_IF Interface

Specify this parameter to display only statistics for the messaging interface you specify. Possible values are 0 and 1.

[-**counter** <text>] - Error Counter Name

Specify this parameter to display only the statistic counter you specify.

[-**value** <integer>] - Error Counter Value

Specify this parameter to display only statistics that have the counter value you specify.

### Examples

---

The following example displays per-interface performance statistics for the storage-failover interconnect on a node named node0a:

```
cluster1::*> storage failover interconnect statistics performance vi-if node0a
Node      Interface  Counter Name                                     Counter Value
node0a    0          Send credit                                     35
node0a    0          Send Queue length                             0
node0a    0          Send Queue full                               0
node0a    0          Sent Queue length                             0
node0a    0          Sent data                                     86868
node0a    0          Receive Queue length                           36
node0a    0          Received data                                 86868
node0a    0          Explicit credit updates received              35
node0a    0          Explicit credit updates sent                 35
node0a    0          Piggyback credit updates received            1143
node0a    0          Piggyback credit updates sent               1142
node0a    0          Sent mbufs                                   1143
node0a    0          Recv mbufs freed by vi_if                     1
node0a    0          Recv mbufs freed by client                   1143
node0a    1          Send credit                                    33
node0a    1          Send Queue length                             0
node0a    1          Send Queue full                               0
node0a    1          Sent Queue length                             1
node0a    1          Sent data                                    12230704
node0a    1          Receive Queue length                           36
node0a    1          Received data                                12230784
node0a    1          Explicit credit updates received              35
node0a    1          Explicit credit updates sent                 35
node0a    1          Piggyback credit updates received            509611
node0a    1          Piggyback credit updates sent               509616
node0a    1          Sent mbufs                                   509613
node0a    1          Recv mbufs freed by vi_if                     509617
node0a    1          Recv mbufs freed by client                     0
```

---

## storage failover internal-options modify

Modify the internal options for storage failover

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

### Description

The `storage failover internal-options modify` command changes some of the storage failover internal options for a node.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node whose storage failover internal options are to be modified.

### Examples

The following example enables failover when the cluster ports are down on a node named node0:

```
node::*> storage failover internal-options modify -node node0 -failover-when-cluster-ports-down true
```

The following example sets the failover to start if node0's cluster ports are down for more than 30 seconds:

```
node::*> storage failover internal-options modify -node node0 -cluster-ports-down-interval 30
```

## storage failover internal-options show

Display the internal options for storage failover

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

### Description

The `storage failover internal-options show` command displays the following information about the storage failover configuration:



- 
- Node name
  - Whether automatic giveback is enabled
  - Whether partner checking is enabled
  - Takeover detection time, in seconds
  - Whether takeover on failover is enabled
  - Whether takeover on panic is enabled
  - Whether takeover on reboot is enabled
  - Whether hardware-assisted takeover is enabled
  - IP address on which the partner node listens to the hardware-assisted takeover alerts
  - Port on which the partner node listens to the hardware-assisted takeover alerts
  - Whether takeover on short uptime is enabled (detailed view only)
  - Short uptime interval, in seconds (detailed view only)
  - Number of giveback attempts (detailed view only)
  - Giveback attempt interval, in minutes (detailed view only)
  - Whether status is propagated through SFO mailboxes (detailed view only)
  - Status read interval, in seconds (detailed view only)
  - Status write interval, in seconds (detailed view only)
  - Hardware-assisted takeover retry count (detailed view only)
  - Hardware-assisted takeover heartbeat period (detailed view only)
  - Whether operator-initiated planned takeover is optimized

## Parameters

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

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

| [-**more** ]

This parameter displays the following additional information: :

- Node name

- 
- Whether takeover on short uptime is enabled
  - Short uptime interval, in seconds
  - Number of giveback attempts
  - Giveback attempt interval, in minutes
  - Whether status is propagated through SFO mailboxes
  - Status read interval, in seconds
  - Status write interval, in seconds
  - Hardware-assisted takeover retry count
  - Hardware-assisted takeover heartbeat period

| [-instance ] }

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

**[-node {<nodename>|local}]** - Node

Selects configuration information for the specified node.

**[-auto-giveback {true|false}]** - Auto Giveback Enabled

Selects configuration information for nodes that have the specified automatic giveback setting.

**[-check-partner {true|false}]** - Check Partner Enabled

Selects configuration information for nodes that have the specified partner-checking setting.

**[-detection-time <integer>]** - Takeover Detection Time (secs)

Selects configuration information for nodes that have the specified takeover detection time setting.

**[-onfailure {true|false}]** - Takeover on Failure Enabled

Selects configuration information for nodes that have the specified takeover-on-failure setting.

**[-onpanic {true|false}]** - Takeover on Panic Enabled

Selects configuration information for nodes that have the specified takeover-on-panic setting.

**[-onshort-uptime {true|false}]** - Takeover on Short Uptime Enabled

---

Selects configuration information for nodes that have the specified takeover-on-short-uptime setting.

**[-short-uptime <integer>]** - Short Uptime (secs)

Selects configuration information for nodes that have the specified takeover-on-short-uptime time setting.

**[-attempts <integer>]** - Number of Giveback Attempts

Selects configuration information for nodes that have the specified number of giveback attempts setting.

**[-attempts-time <integer>]** - Giveback Attempts Minutes

Selects configuration information for nodes that have the specified giveback attempt time setting.

**[-propagate {true|false}]** - Propagate Status via Mailbox

Selects configuration information for nodes that have the specified setting for propagation of status through Storage Failover mailboxes.

**[-read-interval <integer>]** - Node Status Read Interval (secs)

Selects configuration information for nodes that have the specified status read interval setting.

**[-write-interval <integer>]** - Node Status Write Interval (secs)

Selects configuration information for nodes that have the specified status write interval setting.

**[-onreboot {true|false}]** - Takeover on Reboot Enabled

Selects configuration information for nodes that have the specified takeover-on-reboot setting.

**[-delay-seconds <integer>]** - Delay Before Auto Giveback (secs)

If this parameter is specified, the command displays information only about the node or nodes that have the specified delay for auto giveback.

**[-hwassist {true|false}]** - Hwassist Enabled

Selects configuration information for nodes that have the specified hardware-assisted takeover setting.

**[-hwassist-partner-ip <text>]** - Partner's Hwassist IP

Selects configuration information for nodes that have the specified partner IP setting for hardware-assisted takeovers.

---

**[-hwassist-partner-port <integer>]** - Partner's Hwassist Port

Selects configuration information for nodes that have the specified partner port setting for hardware-assisted takeovers.

**[-hwassist-health-check-interval <integer>]** - Hwassist Health Check Interval (secs)

Selects configuration information for nodes that have the specified health check interval setting for hardware-assisted takeovers

**[-hwassist-retry-count <integer>]** - Hwassist Retry Count

Selects configuration information for nodes that have the specified retry count (in seconds) for hardware-assisted takeovers.

**[-mode {ha|non\_ha}]** - HA Mode

If this parameter is specified, the command displays information only about the node or nodes that have the specified HA mode.

**[-bypass-takeover-optimization {true|false}]** - Bypass Takeover Optimization Enabled

Selects configuration information for nodes that have the specified setting for bypass takeover optimization ( true means that optimized operator-initiated planned takeover is bypassed, false means that it is enabled). Operator-initiated planned takeover is optimized when SFO aggregates are relocated serially to the partner prior to takeover. This reduces client outage.

## Examples

The following example displays detailed information about the internal options for storage failover on a node named node2:

```
cluster1::*> storage failover internal-options show -node node2
Node: node2
Auto Giveback Enabled: false
Check Partner Enabled: true
Takeover Detection Time (secs): 15
Takeover On Failure Enabled: true
Takeover On Panic Enabled: false
Takeover On Short Uptime Enabled: true
Short Uptime (secs): -
Number of Giveback Attempts: 3
Giveback Attempts Minutes: 10
Propagate Status Via Mailbox: true
Node Status Read Interval (secs): 5
Node Status Write Interval (secs): 5
Failover the Storage when Cluster Ports Are Down: -
Failover Interval when Cluster Ports Are Down (secs): -
Takeover on Reboot Enabled: true
Delay Before Auto Giveback (secs): 300
Hardware Assist Enabled: true
Partner's Hw-assist IP:
Partner's Hw-assist Port: 4444
Hw-assist Health Check Interval (secs): 180
Hw-assist Retry count: 2
HA mode: ha
Bypass Takeover Optimization Enabled: true
```

---

## storage failover mailbox-disk show

Display information about storage failover mailbox disks

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

### Description

The `storage failover mailbox-disk show` command lists the mailbox disks that are used by storage failover. The command displays the following information:

- Node name
- Whether the mailbox disk is owned by the local node or by its partner
- Disk name
- Disk universal unique identifier (UUID)

This command is available only at the advanced privilege level and higher.

### Parameters

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

If `-fields <fieldname>,...` is used, the command displays only the specified fields.

| **[-instance ]** }

If this parameter is used, the command displays detailed information about all entries.

**[-node** {<nodename>|local}] - Node

Selects the mailbox disks that are associated with the specified node.

**[-location** {local|partner}] - Mailbox Location

Selects the mailbox disks that have the specified relationship to the node.

**[-diskindex** <integer>] - Mailbox Disk Index

Selects the mailbox disk that has the specified index number.

**[-diskname** <text>] - Mailbox Disk Name

Selects the mailbox disks that match the specified disk name. Disk names are specified in the format <host\_adapter>: <loop\_ID>, or <host\_adapter>: <loop\_ID>L <LUN> for a

---

LUN disk. Elsewhere in the system, this format is preceded by the owning node and a colon; however, in the context of this command, the node is listed in its own field.

**[-diskuuid <text>]** - Mailbox Disk UUID

Selects the mailbox disks that match the specified UUID.

### Examples

The following example displays information about the mailbox disks on a node named node1:

```
cluster1::*> storage failover mailbox-disk show -node node1
Node      Location  Index Disk Name      Disk UUID
-----
node1
    local      0 0a.18      20000000:8777E9D6:[...]
    local      1 0a.17      20000000:8777E9DE:[...]
    partner    0 0b.18      20000000:877BA634:[...]
    partner    1 0b.17      20000000:8777C1F2:[...]
```

---

## storage failover progress-table show

Display status information about storage failover operations

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

### Description

The `storage failover progress-table show` displays status information about storage-failover operations. This information is organized in a resource table. The command displays the following information:

- Node name
- Resource-entry index number
- Resource-entry name
- Resource-entry state
- Resource-entry failure code
- Resource-entry time delta

This command is available only at the advanced privilege level and higher.

### Parameters

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

If `-fields <fieldname>, ...` is used, the command will only displays only the specified fields.

| [-**instance** ] }

If this parameter is used, the command displays detailed information about all entries.

[-**node** {<nodename>|local}] - Node

Selects the status information for the specified node.

[-**index** <integer>] - Resource Table Index

Selects the status information for the specified index number.

[-**entryname** <text>] - Resource Table Entry Name

Selects the status information for the specified entry name.

**[-state <text>] - Resource Table Entry State**

Selects the status information for the specified state. Possible values include UP, START\_RUNNING, START\_DONE, START\_FAILED, STOP\_RUNNING, STOP\_FAILED, TAKEOVER\_BARRIER, and ONLY\_WHEN\_INITD.

**[-failurecode <text>] - Entry Failure Code**

Selects the status information for the specified failure code. Possible values include OK, FAIL, FAIL\_ALWAYS, HANG, PANIC, and VETO.

**[-timedelta <integer>] - Entry Time Delta**

Selects the status information for the specified time delta.

**Examples**

The following example displays the entire storage-failover resource table:

```
cluster1::*> storage failover progress-table show
Node   Entry Name                               State      Time Delta
-----
node0
  Pre-rsrctl: fmdisk_resumePartnerDi      start_done      6
  Pre-rsrctl: coredump_get_busy_spar       start_done     107
  Pre-rsrctl: raid_preread_labels_be       start_done      1
  Pre-rsrctl: fmdisk_reserve_all          start_done     84
  rsrctl: fmrsrc_giveback_done             start_done      0
  rsrctl: fmic                             start_done      0
  rsrctl: fmdisk_reserve                   start_done     171
  rsrctl: fm_partnerSlowTimeout            start_done      1
  rsrctl: fmdisk_inventory                 start_done      0
  rsrctl: fmfsm_reserve                    start_done      0
Press <space> to page down, <return> for next line, or 'q' to quit...
Node   Entry Name                               State      Time Delta
-----
node0
  rsrctl: rdb-ha                           start_done     36
  rsrctl: giveback_cleanup_wait            start_done      0
  rsrctl: priority_ha                      start_done      0
  rsrctl: raid                             start_done    113
  rsrctl: raid_disaster_early              start_done      0
  rsrctl: wafn_nvram_replay                start_done      0
  rsrctl: takeover_test_1                  start_done      0
```



---

## storage firmware download

Download disk, ACP Processor and shelf firmware

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

### Description

The `storage firmware download` command downloads ACP processor, disk and shelf firmware to a specified node. The optional parameter `-package-type` is used when downloading a specific firmware file for a single component. If `-package-type` `all` is specified or if not specified, the command assumes that the compressed archive file (.zip) or tarfile contains multiple firmware files that are to be downloaded by the node and includes sub-directory path information for each file.

Use the `storage disk updatefirmware` command to install downloaded disk firmware.

Use the `system node run local storage download shelf` command to install downloaded disk shelf module firmware.

Use the `system node run local storage download acp` command to install downloaded ACP processor firmware.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node to which the firmware is to be downloaded.

**[-package-type** {all|acpp|disk|shelf}] - Type of Firmware Package

This specifies the type of the firmware package. Possible values include `all`, `shelf`, `disk`, and `acpp`. The default value is `all`.

**-package-url** <text> - Package URL

This specifies the path to the firmware package.

The following URL protocols are supported: `ftp`, `http`, and `tftp`.

### Examples

The following example downloads a disk firmware package with the path `ftp://example.com/fw/disk-fw-1.2.zip` to a node named `Cluster1`:

```
Cluster1::> storage firmware download -node node1 -package-type disk
```

---

```
-package ftp://example.com/fw/disk-fw-1.2.zip
```

## See Also

storage disk updatefirmware system node run

---

## storage library config show

Display connectivity to back-end storage libraries.

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

### Description

This command displays information such as how the storage tape libraries connect to the cluster, LUN groups, number of LUNs, WWPN, and switch port information. Use this command to verify the cluster-mode storage tape library configuration or to assist in troubleshooting.

### Parameters

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

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

| [-switch ]

If you specify this parameter, switch port information is shown.

| [-instance ] }

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

**[-node {<nodename>|local}]** - Controller Name

The name of the clustered node for which information is being displayed.

**[-group <integer>]** - LUN Group

A LUN group is a set of LUNs that shares the same path set.

**[-target-wwpn <text>]** - Library Target Ports

The World Wide Port Name of a storage tape library port.

**[-initiator <text>]** - Initiator

The host bus adapter that the clustered node uses to connect to storage tape libraries.

**[-array-name <array name>]** - Library Name

---

Name of the storage tape library that is connected to the clustered node.

**[-target-side-switch-port <text>]** - Target Side Switch Port

This identifies the switch port that connects to the tape library's target port.

**[-initiator-side-switch-port <text>]** - Initiator Side Switch Port

This identifies the switch port that connects to the node's initiator port.

**[-lun-count <integer>]** - Number of LUNS

This is a command-line switch (-lun-count) used to restrict what LUN groups are displayed in the output.

### Examples

The following example displays the storage tape library configuration information.

```
cluster1::> storage library config show
Node      LUN  LUN
Initiator Group Count      Library Name      Library Target Port
-----
cluster1-01 0    2      NEO-0      50050763124b4d6f
3d
cluster1::>
```

---

## storage library path show-by-initiator

Display a list of LUNs on the given Tape Library

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

### Description

This command displays path information for every initiator port connected to a tape library. The output is similar to the `storage library path show` command but the output is listed by initiator.

### Parameters

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

fields used to be used in this display

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Controller name

The name of the clustered node for which information is being displayed.

[-**initiator** <text>] - Initiator Port

Initiator port that the clustered node uses.

[-**target-wwpn** <text>] - Target Port

Target World Wide Port Name. Port on the storage tape library that is being used.

[-**initiator-side-switch-port** <text>] - Initiator Side Switch Port

Switch port connected to the clustered node.

[-**target-side-switch-port** <text>] - Target Side Switch Port

Switch port connected to the tape library.

[-**array-name** <array name>] - Library Name

Name of the storage tape library that is connected to the cluster.

[-**tpgn** <integer>] - Target Port Group Number

TPGN refers to the target port group to which the target port belongs. A target port group is a set of target ports which share the same LUN access characteristics and failover behaviors.

**[-port-speed <text>]** - Port Speed

Port Speed of the specified port.

**[-path-io-kbps <integer>]** - Kbytes of I/O per second on Path (Rolling Average)

Rolling average of Kbytes of I/O per second on the library path.

**[-path-iops <integer>]** - Number of I/O per second on Path (Rolling Average)

Rolling average of I/O per second on the library path.

**[-initiator-io-kbps <integer>]** - Kbytes of I/O per second on Initiator (Rolling Average)

Rolling average of Kbytes of I/O per second on the initiator port.

**[-initiator-iops <integer>]** - Number of I/O per second on Initiator (Rolling Average)

>Rolling average of I/O per second on the initiator port.

**[-target-io-kbps <integer>]** - Kbytes of I/O per second to Target (Rolling Average)

Rolling average of Kbytes of I/O per second on the target port.

**[-target-iops <integer>]** - Number of I/O per second to Target (Rolling Average)

Rolling average of I/O per second on the target port.

## Examples

The following example displays the path information by initiator for a storage tape library.

```
cluster1::> storage library path show-by-initiator
Node: cluster1-01
  Initiator I/O      Initiator Side      Path I/O      Target Side
Initiator      (KB/s)      Target Port      Switch Port      (KB/s)      Switch Port
(KB/s)
-----
0b              0  sw_tape:6              0              sw_tape:0
    0 510a09800000412d NETAPP_VTL_1              sw_tape:1
    0 510a09820000412d NETAPP_VTL_1
3d              0  N/A              0              N/A
    0 50050763124b4d6f NEO-0
3 entries were displayed.
```

---

## storage library path show

Display a list of Tape Libraries on the given path

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

### Description

This command displays path information for a tape library and has the following parameters by default:

- Node name
- Initiator port
- Target port
- TPGN (Target Port Group Number)
- Port speeds
- Path I/O in Kbytes/sec
- IOPs

### Parameters

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

fields used to be used in this display

| [-**detail** ]

Using this option displays the following:

- Target IOPs
- Target LUNs
- Path IOPs
- Path errors
- Path quality
- Path LUNs
- Initiator IOPs

- 
- Initiator LUNs

| [-instance ] }

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

**[-node {<nodename>|local}]** - Controller name

The name of the clustered node for which information is being displayed.

**[-array-name <array name>]** - Library Name

Name of the storage tape library that is connected to the cluster.

**[-target-wwpn <text>]** - Target Port

Target World Wide Port Name. Port on the storage tape library that is being used.

**[-initiator <text>]** - Initiator Port

Initiator port that the clustered node uses.

**[-initiator-side-switch-port <text>]** - Initiator Side Switch Port

Switch port connected to the clustered node.

**[-tpgn <integer>]** - Target Port Group Number

TPGN refers to the target port group to which the target port belongs. A target port group is a set of target ports which share the same LUN access characteristics and failover behaviors.

**[-port-speed <text>]** - Port Speed

Port Speed of the specified port.

**[-path-io-kbps <integer>]** - Kbytes of I/O per second on Path(Rolling Average)

Rolling average of Kbytes of I/O per second on the library path.

**[-path-iops <integer>]** - Number of I/O per second on Path(Rolling Average)

Rolling average of I/O per second on the library path.

**[-initiator-io-kbps <integer>]** - Kbytes of I/O per second on Initiator(Rolling Average)

Rolling average of Kbytes of I/O per second on the initiator port.

**[-initiator-iops <integer>]** - Number of I/O per second on Initiator(Rolling Average)

>Rolling average of I/O per second on the initiator port.

**[-target-io-kbps <integer>]** - Kbytes of I/O per second to Target(Rolling Average)



Rolling average of Kbytes of I/O per second on the target port.

**[-target-iops <integer>]** - Number of I/O per second to Target(Rolling Average)

Rolling average of I/O per second on the target port.

**[-target-side-switch-port <text>]** - Target Side Switch Port

Switch port connected to the tape library.

**[-path-link-errors <integer>]** - Link Error count on path

Fibre Channel link error count.

**[-path-quality <integer>]** - Percentage of weighted error threshold

A number representing the threshold of errors that is allowed on the path. Path quality is a weighted error value. When the error weight of a path exceeds the threshold, I/O is routed to a different path.

**[-path-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this path

Number of LUNs on this path.

**[-initiator-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this initiator

Number of LUNs on this initiator.

**[-target-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this target

Number of LUNs on this target.

## Examples

The following example displays the path information for a storage tape library

```
cluster1::> storage library path show
Node      Initiator  Target Port      TPGN  Speed
(KB/s)
-----
cluster1-01  3d      50050763124b4d6f  61    4 Gb/S
0
cluster1-01  0b      510a09800000412d  35    4 Gb/S
0
cluster1-01  0b      510a09820000412d  1     4 Gb/S
0
3 entries were displayed.
```

---

## storage load balance

Balance storage I/O across controller's initiator ports

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

### Description

This command is obsolete. I/O load is balanced automatically every five minutes.

### Parameters

**-node** {<nodename>|local} - Node to balance on

The name of the clustered node for which information is being displayed.

### Examples

This command has no effect.

---

## storage load show

Display I/O statistics to array LUNs, grouped by initiator port.

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

### Description

The `storage load show` command displays the load distribution of I/O on the cluster.

### Parameters

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

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

| [-**switch** ]

The switch parameter adds switch information to the display.

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Controller name

The name of the clustered node for which information is being displayed.

[-**initiator-port** <text>] - Initiator Port

The initiator port of the array LUN for which I/O stats are being displayed.

[-**wwpn** <text>] - Target Port WWPN

The World Wide Port Name of the array LUN for which I/O stats are being displayed.

[-**serialnumber** <text>] - Serial Number

The serial number of the array LUN for which I/O stats are being displayed.

[-**lun** <integer>] - LUN

The array LUN for which I/O stats are being displayed.

[-**pct-io** <text>] - %I/O

---

Percent of I/O bandwidth consumed by this array LUN.

**[-io-blocks <integer>]** - I/O (blocks)

Number of I/O blocks transferred.

**[-switch-port <text>]** - Switch Port

The initiator side switch port for this array LUN.

**[-target-side-switch-port <text>]** - Target Side Switch Port

The target side switch port for this array LUN.

## Examples

```
vnv3070f3a:> storage load show -switch
Initiator port: 0a connected to vnbr3850s4:7.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					
1	D600020C00D3	0	50060e80004291c0	vnbr3850s5:12	0
2	D600020C00D4	21	50060e80004291c0	vnbr3850s5:12	100
5	D600020C00EF	0	50060e80004291c0	vnbr3850s5:12	0

```
Initiator port: 0c connected to vnci9124s54:1-11.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					
3	D600020C00D9	8	50060e80004291c2	vnci9124s54:1-22	42
4	D600020C00DA	7	50060e80004291c2	vnci9124s54:1-22	36
6	D600020C00F0	3	50060e80004291c2	vnci9124s54:1-22	15

```
Initiator port: 0a connected to vnbr3850s4:8.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					
2	D600020C00D4	0	50060e80004291c0	vnbr3850s5:12	0

```
Initiator port: 0a connected to vnbr3850s4:8.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					
5	D600020C00EF	0	50060e80004291c0	vnbr3850s5:12	0
6	D600020C00F0	31	50060e80004291c0	vnbr3850s5:12	100

```
Initiator port: 0c connected to vnci9124s54:1-12.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					
1	D600020C00D3	0	50060e80004291c2	vnci9124s54:1-22	0

```
Initiator port: 0c connected to vnci9124s54:1-12.
```

LUN	Serial #		Target Port	Target Side Switch Port	%I/O
I/O (blocks)					

---

3	D600020C00D9	50060e80004291c2	vnci9124s54:1-22	42
4	D600020C00DA	50060e80004291c2	vnci9124s54:1-22	42

12 entries were displayed.

---

## storage path quiesce

Quiesce I/O to an array LUN on one path.

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

### Description

The `storage path quiesce` command quiesces I/O on one path to a LUN. After the I/O has been quiesced, no new I/O is sent on the path to the array LUN unless the `storage path resume` command is issued to continue I/O.

### Parameters

**-node** {<nodename>|local} - Node name

The name of the clustered node for which information is being displayed.

**-initiator** <initiator name> - Initiator Port

Initiator port that the clustered node uses.

**-target-wwpn** <wwpn name> - Target Port

Target World Wide Port Name. Port on the storage array that is being used.

**-lun-number** <integer> - LUN Number

Logical Unit number. The range is: [0...65535]

### Examples

The following example suspends I/O between node `vbv3170f1b`, port `0a` and the array port `50001fe1500a8669`, LUN `1`.

```
node::> storage path quiesce -node vbv3170f1b -initiator 0a -target-wwpn
50001fe1500a8669 -lun-number 1
```

### See Also

`storage path resume`

---

## storage path resume

Resume I/O to an array LUN on a path.

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

### Description

The `storage path resume` command continues I/O flow to an array LUN on a path that was previously quiesced. Resuming I/O to a quiesced array LUN is not an error.

### Parameters

**-node** {<nodename>|local} - Node name

The name of the clustered node for which information is being displayed.

**-initiator** <initiator name> - Initiator Port

Initiator port that the clustered node uses.

**-target-wwpn** <wwpn name> - Target Port

Target World Wide Port Name. Port on the storage array that is being used.

**-lun-number** <integer> - LUN Number

Logical Unit number. The range is: [0...65535]

### Examples

The following example quiesces I/O between node vbv3170f1b, port 0a and the array port 50001fe1500a8669, LUN 1

```
node::> storage path resume -node vbv3170f1b -initiator 0a -target-wwpn
50001fe1500a8669 -lun-number 1
```

## storage path show-by-initiator

Display a list of paths to attached arrays from the initiator's perspective

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

---

## Description

The `storage path show-by-initiator` command displays path based statistics. The output is similar to the `storage path show` command but the output is listed by initiator.

## Parameters

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

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

| [-instance ] }

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

**[-node {<nodename>|local}]** - Controller name

The name of the clustered node for which information is being displayed.

**[-initiator <text>]** - Initiator Port

Initiator port that the clustered node uses.

**[-target-wwpn <text>]** - Target Port

Target World Wide Port Name. Port on the storage array that is being used.

**[-initiator-side-switch-port <text>]** - Initiator Side Switch Port

Switch port connected to the clustered node.

**[-target-side-switch-port <text>]** - Target Side Switch Port

Switch port connected to the array.

**[-array-name <array name>]** - Array Name

Name of the storage array that is connected to the cluster.

**[-tpgn <integer>]** - Target Port Group Number

TPGN refers to the target port group to which the target port belongs. A target port group is a set of target ports which share the same LUN access characteristics and failover behaviors.

**[-port-speed <text>]** - Port Speed

Port Speed of the specified port.



**[-path-io-kbps <integer>]** - Kbytes of I/O per second on Path (Rolling Average)

Rolling average of I/O per second on the path.

**[-path-iops <integer>]** - Number of IOPS on Path (Rolling Average)

Rolling average of Kbytes of I/O per second on the path

**[-initiator-io-kbps <integer>]** - Kbytes of I/O per second on Initiator (Rolling Average)

Rolling average of I/O per second on the initiator port.

**[-initiator-iops <integer>]** - Number of IOPS on Initiator (Rolling Average)

Rolling average of Kbytes of I/O per second on the initiator port.

**[-target-io-kbps <integer>]** - Kbytes of I/O per second to Target (Rolling Average)

Rolling average of I/O per second on the target port.

**[-target-iops <integer>]** - Number of IOPS to Target (Rolling Average)

Rolling average of Kbytes of I/O per second on the target port.

## Examples

```
Node: vnv3070f20b      vnv3070f20b::> storage path show-by-initiator
Initiator I/O          Initiator Side    Path I/O          Target Side
Initiator              (KB/s)          Switch Port      (KB/s)          Switch Port
(KB/s)                Target Port Array Name
-----
0a                      3 vnbr3850s4:4          3          vnbr3850s5:15
    3 200600a0b819e16f IBM_1722_1          0          vnbr3850s5:12
    0 50060e80004291c0 HITACHI_DF600F_1
0c                      35 vnci9124s54:1-6      35          vnci9124s54:1-24
    35 200700a0b819e16f IBM_1722_1          0          vnci9124s54:1-22
    0 50060e80004291c2 HITACHI_DF600F_1
4 entries were displayed.
```

## See Also

storage path show

---

## storage path show

Display a list of paths to attached arrays.

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

### Description

The `storage path show` command displays path based statistics. The default command shows:

- Node name
- Initiator port
- Target port
- TPGN
- Port speeds
- Path I/O in Kbytes/sec
- IOPs

### Parameters

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

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

| [-**array** ]

Using this option displays:

- Array name
- Target port
- Target I/O in Kbytes/sec
- Target side switch port
- Path I/O in Kbytes/sec
- Initiator side switch port

- 
- Initiator I/O in Kbytes/sec
  - Initiator port

| **[-by-target ]**

Using this option displays the same information as the array option, but grouped by target port.

| **[-detail ]**

Using this option displays the same information as the array and by-target options, but adds the following:

- Target IOPs
- Target LUNs
- Path IOPs
- Path errors
- Path quality
- Path LUNs
- Initiator IOPs
- Initiator LUNs

| **[-switch ]**

Using this option adds switch port information to the default display.

| **[-instance ] }**

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

**[-node {<nodename>|local}]** - Controller name

The name of the clustered node for which information is being displayed.

**[-array-name <array name>]** - Array Name

Name of the storage array that is connected to the cluster.

**[-target-wwpn <text>]** - Target Port

Target World Wide Port Name. Port on the storage array that is being used.

**[-initiator <text>]** - Initiator Port

Initiator port that the clustered node uses.

---

**[-initiator-side-switch-port <text>]** - Initiator Side Switch Port

Switch port connected to the clustered node.

**[-tpgn <integer>]** - Target Port Group Number

TPGN refers to the target port group to which the target port belongs. A target port group is a set of target ports which share the same LUN access characteristics and failover behaviors.

**[-port-speed <text>]** - Port Speed

Port Speed of the specified port.

**[-path-io-kbps <integer>]** - Kbytes of I/O per second on Path (Rolling Average)

Rolling average of I/O per second on the path.

**[-path-iops <integer>]** - Number of IOPS on Path (Rolling Average)

Rolling average of Kbytes of I/O per second on the path

**[-initiator-io-kbps <integer>]** - Kbytes of I/O per second on Initiator (Rolling Average)

Rolling average of I/O per second on the initiator port.

**[-initiator-iops <integer>]** - Number of IOPS on Initiator (Rolling Average)

Rolling average of Kbytes of I/O per second on the initiator port.

**[-target-io-kbps <integer>]** - Kbytes of I/O per second to Target (Rolling Average)

Rolling average of I/O per second on the target port.

**[-target-iops <integer>]** - Number of IOPS to Target (Rolling Average)

Rolling average of Kbytes of I/O per second on the target port.

**[-target-side-switch-port <text>]** - Target Side Switch Port

Switch port connected to the array.

**[-path-link-errors <integer>]** - Link Error count on path

Fibre Channel link error count.

**[-path-quality <integer>]** - Percentage of weighted error threshold

A number representing the threshold of errors that is allowed on the path. Path quality is a weighted error value. When the error weight of a path exceeds the threshold, I/O is routed to a different path.

**[-path-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this path

Number of LUNs on this path.

---

**[-initiator-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this initiator

Number of LUNs on this initiator.

**[-target-lun-in-use-count <integer>]** - Number of LUNs in the in-use state on this target

Number of LUNs on this target.

## Examples

The following example shows the default display.

```
vbv3170f2a::> storage path show
```

Path Node (KB/s)	I/O IOPS	Initiator	Array Target Port	TPGN	Speed
vbv3170f2a-01	6	0b	50001fe1500a866c	2	2 Gb/S
vbv3170f2a-01	0	0b	50001fe1500a866d	2	2 Gb/S
vbv3170f2a-01	0	0c	50001fe1500a866e	4	4 Gb/S
vbv3170f2b-03	3	0a	50001fe1500a866d	1	2 Gb/S
vbv3170f2b-03	3	0c	50001fe1500a866f	4	4 Gb/S

5 entries were displayed.

The following example shows how the information is displayed with the array option.

```
Node: vnv3070f20b vnv3070f20b::> storage path show -array
```

Array Name	Initiator Side Switch Port	Initiator I/O Target Port (KB/s)	Target I/O Initiator (KB/s) Port	Target Side Switch Port	Path I/O (KB/s)
HITACHI_DF600F_1	50060e80004291c0	3	0a	0	0
vnbr3850s4:4	50060e80004291c2	26	0c	0	0
vnbr3850s4:4	50060e80004291c2	26	0c	0	0
IBM_1722_1	200600a0b819e16f	3	0a	3	3
vnbr3850s4:4	200700a0b819e16f	26	0c	26	26
vnbr3850s4:4	200700a0b819e16f	26	0c	26	26

4 entries were displayed.

The following example shows how the information is displayed when grouped by target.

```
Node: vnv3070f20b vnv3070f20b::> storage path show -by-target
```

Array Name	Initiator Side Switch Port	Initiator I/O Target Port (KB/s)	Target I/O Initiator (KB/s) Port	Target Side Switch Port	Path I/O (KB/s)	Initiator Switch
HITACHI_DF600F_1	50060e80004291c0	3	0a	0	0	
vnbr3850s4:4	50060e80004291c2	26	0c	0	0	

```

50060e80004291c2          0      vnci9124s54:1-22          0
vnci9124s54:1-6          26      0c
Node: vnv3070f20b
Array Name: IBM_1722_1
      Target I/O          Target Side          Path I/O          Initiator
Side Initiator I/O Initiator          Switch Port          (KB/s)          Switch
Target Port          (KB/s)          Port
Port          (KB/s)          Port
-----
200600a0b819e16f          3      vnbr3850s5:15          3
vnbr3850s4:4          3      0a
200700a0b819e16f          26      vnci9124s54:1-24          26
vnci9124s54:1-6          26      0c
4 entries were displayed.

```

The following example shows how the information is displayed with the switch option.

```

vbv3170f2b::> storage path show -switch
      Target Side
Initiator Side          Path I/O          Target Side
Node          Initiator          Array Target Port          Switch Port
Switch Port          TPGN          Speed          (KB/s)          IOPS
-----
vbv3170f2a-01          0b          50001fe1500a866c          vbbr300s1:6
vbbr300s1:2          2      2      Gb/S          9      3
vbv3170f2a-01          0b          50001fe1500a866d          vbbr300s1:7
vbbr300s1:2          2      2      Gb/S          0      0
vbv3170f2a-01          0c          50001fe1500a866e          vbc9124s2:1-7
vbc9124s2:1-3          4      4      Gb/S          0      0
vbv3170f2b-03          0a          50001fe1500a866d          vbbr300s1:7
vbbr300s1:3          1      2      Gb/S          4      1
vbv3170f2b-03          0c          50001fe1500a866f          vbc9124s2:1-8
vbc9124s2:1-4          4      4      Gb/S          4      1
5 entries were displayed.

```

---

## storage raid-options modify

Modify the dblade option. Extreme care must be taken when making modifications here.

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

### Description

The `storage raid-options modify` command is used to modify the available raid-options for each node in a cluster. Extreme care must be taken while making the modifications.

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node on which the RAID option is to be modified.

**-name** <text> - Options Name

This parameter specifies the RAID option to be modified. To see the list of RAID options that can be modified, use the `storage raid-options show` command.

**[-value <text>]** - Options Value

This parameter specifies the value of the selected RAID option.

### Examples

The following example sets the raid scrub duration to 12 hours for a node named node1:

```
cluster1::*> storage raid-options modify -node node1 -name raid.scrub.duration -  
value 720
```

### See Also

`storage raid-options show`   `storage raid-options`

---

# storage raid-options show

Display a select group of the dblade options

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

## Description

The `storage raid-options show` command displays information about all the raid-options in a cluster.

## Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Selects information about all the raid-options on the specified node.

[-name <text>] - Options Name

Selects information about the raid-options that have the specified name.

[-value <text>] - Options Value

Selects information about all the raid-options that have the specified value.

[-constraint <text>] - Option Constraint

Selects information about all the raid-options that have the specified constraint.

## Examples

The following example shows the raid scrub settings for a node named node1:

```
cluster1::*> storage raid-options show -node node1 -name raid.scrub*
Node   Option                                     Value   Constraint
-----
node1  raid.scrub.duration                       360     none
node1  raid.scrub.enable                         on       none
```



---

node1	raid.scrub.perf_impact	low	only_one
node1	raid.scrub.schedule		none
4 entries were displayed.			

## See Also

storage raid-options

---

## system configuration backup copy

Copy a configuration backup

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

### Description

The `system configuration backup copy` command copies a configuration backup from one node in the cluster to another node in the cluster.

Use the `system configuration backup show` command to display configuration backups to copy.

### Parameters

**-from-node** {<nodename>|local} - Source Node

Use this parameter to specify the name of the source node where the configuration backup currently exists.

**-backup** <text> - Backup Name

Use this parameter to specify the name of the configuration backup file to copy.

**-to-node** {<nodename>|local} - Destination Node

Use this parameter to specify the name of the destination node where the configuration backup copy is created.

### Examples

The following example copies the configuration backup file `node1.special.7z` from the node `node1` to the node `node2`.

```
cluster1::*> system configuration backup copy -from-node node1 -backup
node1.special.7z -to-node node2
[Job 295] Job is queued: Copy backup job.
```

### See Also

`system configuration backup show`

---

## system configuration backup create

Create a configuration backup

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

### Description

The `system configuration backup create` command creates a new configuration backup file.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node on which to create the backup file.

**[-backup-name <text>]** - Backup Name

Use this parameter to specify the name of the backup file to create.

**[-backup-type {node|cluster}]** - Backup Type

Use this parameter to specify the type of backup file to create.

### Examples

The following example creates a new cluster configuration backup file called `node1.special.7z` on the node `node1`.

```
cluster1::*> system configuration backup create -node node1 -backup-name
node1.special.7z -backup-type cluster
[Job 194] Job is queued: Cluster Backup OnDemand Job.
```

---

## system configuration backup delete

Delete a configuration backup

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

### Description

The `system configuration backup delete` command deletes a saved configuration backup.

Use the `system configuration backup show` command to display saved configuration backups.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the source node where the configuration backup currently exists.

**-backup** <text> - Backup Name

Use this parameter to specify the name of the configuration backup file to delete.

### Examples

The following example shows how to delete the configuration backup file `node1.special.7z` from the node `node1`.

```
cluster1::*>system configuration backup delete -node node1 -backup  
node1.special.7z
```

### See Also

`system configuration backup show`

---

## system configuration backup download

Download a configuration backup

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

### Description

The `system configuration backup download` command copies a configuration backup from a source URL to a node in the cluster.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node to which the configuration backup is downloaded.

**-source** <text> - Source URL

Use this parameter to specify the source URL of the configuration backup to download.

**[-backup-name <text>]** - Backup Name

Use this parameter to specify a new local file name for the downloaded configuration backup.

### Examples

The following example shows how to download a configuration backup file from a URL to a file named `exampleconfig.download.7z` on the node `node2`.

```
cluster1::*> system configuration backup download -node node2 -source
http://www.example.com/config/download/nodeconfig.7z -backup-name
exampleconfig.download.7z
```

---

## system configuration backup rename

Rename a configuration backup

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

### Description

The `system configuration backup rename` command changes the file name of a configuration backup file.

Use the `system configuration backup show` command to display configuration backups to rename.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the source node where the configuration backup currently exists.

**-backup** <text> - Backup Name

Use this parameter to specify the name of the configuration backup file to rename.

**-new-name** <text> - New Name

Use this parameter to specify a new name for the configuration backup file.

### Examples

The following example renames the saved configuration file `download.config.7z` on the node `node1` to `test.config.7z`.

```
cluster1::*> system configuration backup rename -node node1 -backup  
download.config.7z -new-name test.config.7z
```

### See Also

`system configuration backup show`

---

## system configuration backup show

Show configuration backup information

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

### Description

The `system configuration backup show` command displays information about saved configuration backups.

### Parameters

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

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

| [-instance ] }

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

**[-node {<nodename>|local}]** - Node

Selects configuration backups that are saved on the node you specify.

**[-backup <text>]** - Backup Name

Selects configuration backups that have the backup name you specify.

**[-backup-type {node|cluster}]** - Backup Type

Selects configuration backups of the type you specify.

**[-time <MM/DD HH:MM:SS>]** - Backup Creation Time

Selects configuration backups that were saved on the date and time you specify.

**[-cluster-name <text>]** - Cluster Name

Selects configuration backups that were saved in the cluster that has the name you specify.

**[-cluster-uuid <UUID>]** - Cluster UUID

---

Selects configuration backups that were saved in the cluster that has the UUID you specify.

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

Selects configuration backups that have the file size you specify.

**[-nodes-in-backup {<nodename>|local}, ...]** - Nodes In Backup

Selects configuration backups that include the configuration of the nodes you specify.

**[-version <text>]** - Software Version

Selects configuration backups that have the software version you specify.

**[-is-auto {true|false}]** - Backup Created from Schedule (true or false)

A value of true selects configuration backups that were created from a schedule. A value of false selects configuration backups that were created manually.

**[-schedule <text>]** - Name of Backup Schedule

Selects configuration backups that were created by the schedule you specify.

## Examples

The following example shows typical output for this command.

```
cluster1::*> system configuration backup show
Node      Backup Tarball                               Time                               Size
-----
node1     cluster1.8hour.2011-02-22.18_15_00.7z       02/22 18:15:00                     7.78MB
node1     cluster1.8hour.2011-02-23.02_15_00.7z       02/23 02:15:00                     7.98MB
node1     cluster1.8hour.2011-02-23.10_15_00.7z       02/23 10:15:00                     7.72MB
node1     cluster1.daily.2011-02-22.00_10_00.7z       02/22 00:10:00                     7.19MB
node1     cluster1.daily.2011-02-23.00_10_00.7z       02/23 00:10:00                     7.99MB
Press <space> to page down, <return> for next line, or 'q' to quit... q
5 entries were displayed.
```



---

## system configuration backup upload

Upload a configuration backup

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

### Description

The `system configuration backup upload` command copies a configuration backup from a node in the cluster to a remote URL.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node from which the configuration backup is uploaded.

**-backup** <text> - Backup Name

Use this parameter to specify the file name of the configuration backup to upload.

**-destination** <text> - Destination URL

Use this parameter to specify the destination URL of the configuration backup.

### Examples

The following example show how to upload the configuration backup file `testconfig.7z` from the node `node2` to a remote URL.

```
cluster1::*> system configuration backup upload -node node2 -backup testconfig.7z  
-destination ftp://www.example.com/config/uploads/testconfig.7z
```

## system configuration backup settings modify

Modify configuration backup settings

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

### Description

---

The `system configuration backup settings modify` command changes settings for configuration backup.

## Parameters

**[-destination <text>]** - Backup Destination URL

Use this parameter to specify the destination URL for uploads of configuration backups. Use the value "" to remove the destination URL.

**[-username <text>]** - Username for Destination

Use this parameter to specify the user name to use to log in to the destination system and perform the upload. Use the `system configuration backup settings set-password` command to change the password used with this user name.

**[-numbackups1 <integer>]** - Number of Backups to Keep for Schedule 1

Use this parameter to specify the number of backups created by backup schedule 1 to keep on the destination system. If the number of backups exceeds this number, the oldest backup is removed.

**[-numbackups2 <integer>]** - Number of Backups to Keep for Schedule 2

Use this parameter to specify the number of backups created by backup schedule 2 to keep on the destination system. If the number of backups exceeds this number, the oldest backup is removed.

**[-numbackups3 <integer>]** - Number of Backups to Keep for Schedule 3

Use this parameter to specify the number of backups created by backup schedule 3 to keep on the destination system. If the number of backups exceeds this number, the oldest backup is removed.

## Examples

The following example shows how to set the destination URL and user name used for uploads of configuration backups.

```
cluster1::*> system configuration backup settings modify -destination ftp://  
www.example.com/config/uploads/ -username admin
```

## See Also

`system configuration backup settings set-password`

---

## system configuration backup settings set-password

Modify password for destination URL

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

### Description

The `system configuration backup settings set-password` command sets the password used for uploads of configuration backups. This password is used along with the username you specify using the `system configuration backup settings modify` command to log in to the system and perform the upload. Enter the command without parameters. The command prompts you for a password, and for a confirmation of that password. Enter the same password at both prompts. The password is not displayed.

Use the `system configuration backup settings show` command to display the destination URL for configuration backups. Use the `system configuration backup settings modify` command to change the destination URL and remote username for configuration backups.

### Parameters

None

### Examples

The following example shows successful execution of this command.

```
cluster1::*> system configuration backup settings set-password
Enter the password:
Confirm the password:
```

### See Also

`system configuration backup settings modify`  
`system configuration backup settings show` `system configuration backup upload`

---

## system configuration backup settings show

Show configuration backup settings

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

### Description

The `system configuration backup settings show` command displays current settings for configuration backup. These settings apply to backups created automatically by schedules. By default, the command displays the URL to which configuration backups are uploaded, and the user name on the remote system used to perform the upload.

Use the `system configuration backup settings set-password` command to change the password used with the user name on the destination. Use the `system configuration backup settings modify` command to change the destination URL and username for uploads of configuration backups, and to change the number of backups to keep for each schedule.

### Parameters

**[-instance ]**

Use this parameter to display detailed information about configuration backup settings, including the number of backups to keep for each backup schedule.

### Examples

The following example displays basic backup settings information.

```
cluster1::*> system configuration backup settings show
Backup Destination URL      Username
-----
ftp://www.example.com/config/uploads/  jdoe
```

The following example shows detailed output using the `-instance` parameter.

```
cluster1::*> system configuration backup settings show -instance
Backup Destination URL: ftp://www.example.com/config/uploads/
Username for Destination: admin
Schedule 1: 8hour
Number of Backups to Keep for Schedule 1: 2
Schedule 2: daily
Number of Backups to Keep for Schedule 2: 2
Schedule 3: weekly
Number of Backups to Keep for Schedule 3: 2
```

---

## See Also

system configuration backup settings set-password  
system configuration backup settings modify

---

## system configuration recovery cluster recreate

Recreate cluster

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

### Description

The `system configuration recovery cluster recreate` command re-creates a cluster, using either the current node or a configuration backup as a configuration template. After you re-create the cluster, rejoin nodes to the cluster using the `system configuration recovery cluster rejoin` command.

### Parameters

**-from {node|backup}** - From Node or Backup

Use this parameter with the value `node` to re-create the cluster using the current node as a configuration template. Use this parameter with the value `backup` to re-create the cluster using a configuration backup as a configuration template.

**[-backup <text>]** - Backup Name

Use this parameter to specify the name of a configuration backup file to use as a configuration template. If you specified the `-from` parameter with the value `backup`, you must use this parameter and specify a backup name. Use the `system configuration backup show` command to view available configuration backup files.

### Examples

The following example shows how to re-create a cluster using the node `node1` as a configuration template.

```
cluster1::*>system configuration recovery cluster recreate -from node
```

The following example shows how to re-create a cluster using the configuration backup `siteconfig.backup.7z` as a configuration template.

```
cluster1::*>system configuration recovery cluster recreate -from backup -backup  
siteconfig.backup.7z
```

### See Also

`system configuration backup show`   `system configuration recovery cluster rejoin`

---

## system configuration recovery cluster rejoin

Rejoin a cluster

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

### Description

The `system configuration recovery cluster rejoin` command rejoins a node to a new cluster created earlier using the `system configuration recovery cluster recreate` command. Only use this command to recover a node from a disaster. Because this synchronization can overwrite critical cluster information, and will restart the node you specify, you are required to confirm this command before it executes.

### Parameters

**-node** {<nodename>|local} - Node to Rejoin

Use this parameter to specify the node to rejoin to the cluster.

### Examples

This example shows how to rejoin the node `node2` to the cluster.

```
cluster1::*> system configuration recovery cluster rejoin -node node2
Warning: This command will rejoin node "node2" into the local cluster,
         potentially overwriting critical cluster configuration files. This
         command should only be used to recover from a disaster. Do not perform
         any other recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

### See Also

`system configuration recovery cluster recreate`

---

## system configuration recovery cluster sync

Sync a node with cluster configuration

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

### Description

The `system configuration recovery cluster sync` command synchronizes a node with the cluster configuration. Only use this command to recover a node from a disaster. Because this synchronization can overwrite critical cluster information, and will restart the node you specify, you are required to confirm this command before it executes.

### Parameters

**-node** {<nodename>|local} - Node to Synchronize

Use this parameter to specify the name of the node to synchronize with the cluster.

### Examples

The following example shows the synchronization of the node `node2` to the cluster configuration.

```
cluster1::*> system configuration recovery cluster sync -node node2
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster configuration
files on the node. This feature should only be used to recover from a
disaster. Do not perform any other recovery operations while this
operation is in progress. This command will cause all the cluster
applications on node "node2" to restart, interrupting administrative
CLI and Web interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that the
cluster applications go online.
```



---

## system configuration recovery node restore

Restore node configuration from a backup

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

### Description

The `system configuration recovery node restore` command restores the configuration of the local node from a configuration backup file.

Use the `system configuration backup show` command to view available configuration backup files.

### Parameters

**-backup** <text> - Backup Name

Use this parameter to specify the name of a configuration backup file to use as the configuration template.

**[-nodename-in-backup** <text>] - Use Backup Identified by this Nodename

Use this parameter to specify a node within the configuration backup file to use as a configuration template. Only specify this parameter if you are specifying a name other than the name of the local node.

**[-force** [true]] - Force Restore Operation

Use this parameter with the value `true` to force the restore operation and overwrite the current configuration of the local node. This overrides all compatibility checks between the node and the configuration backup. The configuration in the backup is installed even if it is not compatible with the node's software and hardware.

Use this parameter with the value `false` to be warned of the specific dangers of restoring and be prompted for confirmation before executing the command. This value also assures that the command performs compatibility checks between configuration stored in the backup and the software and hardware of the node. The default is `false`.

### Examples

The following example shows how to restore the configuration of the local node from the configuration backup of `node3` that is stored in the configuration backup file `example.backup.7z`.

```
cluster1::*> system configuration recovery node restore -backup example.backup.7z
```

---

Warning: This command overwrites local configuration files with files contained in the specified backup file. Use this command only to recover from a disaster that resulted in the loss of the local configuration files. The node will reboot after restoring the local configuration.

Do you want to continue? {y|n}: y

## See Also

system configuration backup show

---

## system health alert delete

Delete system health alert

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

### Description

The `system health alert delete` command deletes all the alerts on the cluster with the specified input parameters.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to delete alerts generated on a cluster only on the node you specify.

**-monitor** <hm\_type> - Monitor

Use this parameter to delete alerts generated on a cluster only on the monitor you specify.

**-alert-id** <text> - Alert ID

Use this parameter to delete alerts generated on a cluster only on the alert ID you specify.

**-alerting-resource** <text> - Alerting Resource

Use this parameter to delete alerts generated on a cluster on the alerting resource you specify.

### Examples

This example shows how to delete an alert with the specified alert-id:

```
cluster1::> system health alert delete -alert-id  
DualPathToDiskShelf_Alert -alerting-resource *
```

## system health alert modify

Modify system health alert

---

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

## Description

The `system health alert modify` command suppresses alerts generated on the cluster and sets the acknowledgement state for an alert.

## Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node on which you want to change the state.

**-monitor** <hm\_type> - Monitor

Use this parameter to specify the monitor name on which you want to change the state.

**-alert-id** <text> - Alert ID

Use this parameter to specify the alert ID on which you want to change the state.

**-alerting-resource** <text> - Alerting Resource

Use this parameter to specify the alerting resource name on which you want to change the state.

**[-acknowledge {true|false}]** - Acknowledge

Use this parameter to set the acknowledgement state to true or false.

**[-suppress {true|false}]** - Suppress

Use this parameter to set the suppress state to true or false.

**[-acknowledger <text>]** - Acknowledger

Use this parameter to set the acknowledgedger as the filter for setting state.

**[-suppressor <text>]** - Suppressor

Use this parameter to set the suppressor as the filter for setting state.

## Examples

This example modifies the alert field states on the cluster:

```
cluster1::> system health alert modify -node * -alert-id  
DualPathToDiskShelf_Alert -suppress true
```

---

## system health alert show

View system health alerts

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

### Description

The `system health alert show` command displays information about all the alerts generated on the system. Using `-instance` will add detailed information.

### Parameters

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

Selects the fields that you specify.

| **[-instance** ] }

Displays the following additional information about each alert:

- Node name
- Resource name
- Severity of the alert
- Probable cause for the alert
- Possible effect due to the alert
- Recommended corrective actions to be followed

**[-node** {<nodename>|local}] - Node

Selects the alerts generated for the specified node.

**[-monitor** <hm\_type>] - Monitor

Selects the alerts with the specified monitor name.

**[-alert-id** <text>] - Alert ID

Selects the alerts with the specified alert ID.

**[-alerting-resource** <text>] - Alerting Resource

Selects the alerts with the specified alerting resource name.

---

**[-subsystem <hm\_subsystem>]** - Subsystem

Selects the alerts generated on the monitoring subsystem.

**[-indication-time <Date>]** - Indication Time

Selects the alerts with the specified indicated time.

**[-perceived-severity <hm\_perceived\_sev>]** - Perceived Severity

Selects the alerts with the perceived severity level.

**[-probable-cause <hm\_probable\_cause>]** - Probable Cause

Selects the alerts that contain the specified probable cause.

**[-probable-cause-description <text>]** - Description

Selects the alerts containing the specified probable cause description.

**[-corrective-actions <text>]** - Corrective Actions

Selects the alerts with the specified recommended corrective action.

**[-possible-effect <text>]** - Possible Effect

Selects the alerts with the specified possible effect.

**[-acknowledge {true|false}]** - Acknowledge

Selects the alerts with the specified acknowledgement status.

**[-suppress {true|false}]** - Suppress

Selects the alerts with the specified suppressor field status of true or false.

**[-policy <text>]** - Policy

Selects the alerts with the specified policy name.

**[-acknowledger <text>]** - Acknowledger

Selects the alerts with the specified acknowledger field.

**[-suppressor <text>]** - Suppressor

Selects the alerts with the specified suppressor field.

**[-additional-info <text>, ...]** - Additional Information

Selects the alerts with the specified additional information.

**[-alerting-resource-name <text>]** - Alerting Resource Name

Selects the alerts with the specified alerting resource name.

---

**[`-tags` <hm\_alert\_type>, ...] - Additional Alert Tags**

Selects the alerts with the specified keywords.

## Examples

The example below displays information about all the alerts generated in the cluster:

```
cluster1::> system health alert show

Node: node1
Resource: Shelf ID 2
Severity: Major
Tags: quality-of-service, nondisruptive-upgrade
Probable Cause: Disk shelf 2 does not have two paths to controller
node1.
Possible Effect: Access to disk shelf 2 via controller node1 will be
lost with a single hardware component failure (e.g.
cable, HBA, or IOM failure).
Corrective Actions: 1. Halt controller node1 and all controllers attached to
disk shelf 2.
following the rules 2. Connect disk shelf 2 to controller node1 via two paths
in the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
```

The example below displays additional information about a specific alert generated in the cluster:

```
cluster1::> system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance

Node: node1
Monitor: node-connect
Alert ID: DualPathToDiskShelf_Alert
Alerting Resource: 50:05:0c:c1:02:00:0f:02
Subsystem: SAS-connect
Indication Time: Mon Mar 21 10:26:38 2011
Perceived Severity: Major
Probable Cause: Connection_establishment_error
Description: Disk shelf 2 does not have two paths to controller node1.
Corrective Actions: 1. Halt controller node1 and all controllers attached to
disk shelf 2.
following the rules in 2. Connect disk shelf 2 to controller node1 via two paths
the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
Possible Effect: Access to disk shelf 2 via controller node1 will be lost
with a single hardware component failure (e.g. cable, HBA, or IOM failure).
Acknowledge: false
Suppress: false
Policy: DualPathToDiskShelf_Policy
Acknowledger: -
Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
Shelf id: 2
Shelf Name: 4d.shelf2
Number of Paths: 1
Number of Disks: 6
Adapter connected to IOMA:
Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
Additional Alert Tags: quality-of-service, nondisruptive-upgrade
```

---

## system health alert definition show

Display system health alert definition

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

### Description

The `system health alert definition show` command displays information about the various alerts defined in the system health monitor policy file. Using `-instance` will display additional details.

### Parameters

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

Selects the fields that you specify.

| **[-instance** ] }

Use this parameter to display additional information on each alert definition.

- Node name
- Monitor name
- Subsystem identifier
- Alert ID
- Severity of the alert
- Probable cause
- Probable cause description
- Possible effect due the error state
- Recommended corrective actions to be followed
- Any additional information
- Additional alert tags

**[-node** {<nodename>|local}] - Node

Selects the alert definitions for the specified node.



---

**[-monitor <hm\_type>]** - Monitor

Selects the alert definitions with the specified monitor name.

**[-alert-id <text>]** - Class of Alert

Selects the alert definitions with the specified alert identifier.

**[-perceived-severity <hm\_perceived\_sev>]** - Severity of Alert

Selects the alert definitions with the specified perceived severity.

**[-probable-cause <hm\_probable\_cause>]** - Probable Cause

Selects the alert definitions with the specified probable cause of the alert.

**[-probable-cause-description <text>]** - Probable Cause Description

Selects the alert definitions with the specified probable cause description.

**[-possible-effect <text>]** - Possible Effect

Selects the alert definitions with the specified possible effect.

**[-corrective-actions <text>]** - Corrective Actions

Selects the alert definitions with the specified corrective action.

**[-subsystem <hm\_subsystem>]** - Subsystem Name

Selects the alert definitions with the specified subsystem.

**[-additional-information <text>]** - Additional Relevant Data

Selects the alert definitions with the specified additional information.

**[-tags <hm\_alert\_type>, ...]** - Additional Alert Tags

Selects the alert definitions with the specified keywords.

## Examples

The example below displays information about all the definitions in the alert definition file:

```
cluster1::> system health alert definition show
Node      Monitor      Subsystem      Alert ID
-----
node-01    system-connect    SAS-connect    DualControllerNonHa_
                        Severity: Major
                        Probable Cause: Configuration_error
Probable Cause Description: Disk shelf $(sschm_shelf_info.id) is connected to
                        two controllers
                        ($ (sschm_shelf_info.connected-nodes)) that are
                        not an HA pair.
                        Possible Effect: Access to disk shelf $(sschm_shelf_info.id) may
                        be lost with a single controller failure.
```

---

```
Corrective Actions: 1. Halt all controllers that are connected to disk
shelf ${sschm_shelf_info.id}).
2. Connect disk shelf ${sschm_shelf_info.id} to both
HA controllers following the rules in the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
Additional Info: -
Tags: quality_of_service, nondisruptive-upgrade
```

The example below displays detailed information about the definitions in the alert definition file:

```
cluster1::> system health alert definition show -instance

Node: krivC-01
Monitor: system-connect
Class of Alert: DualControllerNonHa_Alert
Severity of Alert: Major
Probable Cause: Configuration_error
Probable Cause Description: Disk shelf ${sschm_shelf_info.id} is connected to two
controllers (${sschm_shelf_info.connected-nodes}) that are not an HA pair.
Possible Effect: Access to disk shelf ${sschm_shelf_info.id} may be
lost with a single controller failure.
Corrective Actions: 1. Halt all controllers that are connected to disk
shelf ${sschm_shelf_info.id}).
2. Connect disk shelf ${sschm_shelf_info.id} to
both HA controllers following the rules in the Universal SAS and ACP Cabling
Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert
persists.
Subsystem Name: SAS-connect
Additional Relevant Data: -
Additional Alert Tags: quality_of_service, nondisruptive-upgrade
```

---

## system health autosupport trigger history show

View system health alert history

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

### Description

The `system health autosupport trigger history show` command displays all the alert triggers in the cluster that generated the AutoSupport messages. The following fields are displayed in the output:

- Node name
- Monitor name
- Subsystem
- Alert identifier
- Alerting resource
- Severity
- If an AutoSupport has been sent due to this alert

### Parameters

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

Use this parameter to display only the fields you specify.

| [-**instance** ] }

Use this parameter to display additional information about all of the alerts that were generated.

[-**node** {<nodename>|local}] - Node

Use this parameter to display AutoSupport trigger history on the specified node.

[-**monitor** <hm\_type>] - Monitor

Use this parameter to display AutoSupport trigger history with the specified monitor name.

[-**alert-id** <text>] - Alert ID

Use this parameter to display the AutoSupport message that was triggered by the specified alert ID.

**[-alerting-resource <text>]** - Alerting Resource

Use this parameter to display the AutoSupport message that was triggered by the specified alerting resource.

**[-subsystem <hm\_subsystem>]** - Subsystem

Use this parameter to display the AutoSupport message that was triggered by the specified subsystem.

**[-indication-time <Date>]** - Indication Time

Use this parameter to display the AutoSupport message that was triggered at the indicated time.

**[-perceived-severity <hm\_perceived\_sev>]** - Perceived Severity

Use this parameter to display the AutoSupport message that was triggered by alerts with the specified perceived severity.

**[-autosupport-triggered {true|false}]** - AutoSupport Triggered

Use this parameter to display the alerts that generated AutoSupport messages.

**[-probable-cause <hm\_probable\_cause>]** - Probable Cause

Use this parameter to display the alerts that were generated with the specified probable cause.

**[-corrective-actions <text>]** - Corrective Actions

Use this parameter to display the AutoSupport alerts with the specified corrective actions.

**[-asup-enable {true|false}]** - Enable asup for this alert

Use this parameter to enable or disable an AutoSupport message for this alert.

## Examples

This example displays information about the AutoSupport trigger history

```
cluster1::> system health autosupport trigger history show
Node      Monitor      Subsystem      Alert ID
-----
node1     node-connect  SAS-connect    DualPathToDiskShelf_
                Resource: 50:05:0c:c1:02:00:0f:02
                Severity: Major
                AutoSupport sent: true
```

This example displays info about the autosupport trigger history in detail

---

```
cluster1::> system health autosupport trigger history show -instance
      Node: node1
      Monitor: node-connect
      Alert ID: DualPathToDiskShelf_Alert
Alerting Resource: 50:05:0c:cl:02:00:0f:02
      Subsystem: SAS-connect
      Indication Time: Thu Mar 17 11:59:09 2011
Perceived Severity: Major
AutoSupport Triggered: true
      Probable Cause: Connection_establishment_error
Corrective Actions: 1. Halt controller node1 and all controllers attached to
disk shelf 2.
2. Connect disk shelf 2 to controller node1 via two paths following the rules in
the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
```

---

## system health cluster-switch create

Add information about a cluster switch or management switch

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

### Description

The `system health cluster-switch create` command adds information about a cluster switch or management switch. The cluster switch health monitor uses this information to monitor the health of the switch.

Use this command if Data ONTAP cannot automatically discover a cluster or management switch. Data ONTAP relies on discovery protocols to discover the switches. By default, Data ONTAP automatically attempts to discover and monitor supported cluster and management switches.

If the Cisco Discovery Protocol v1(CDPv1) Daemon is disabled, Data ONTAP cannot discover the cluster and management switches. To verify whether the discovery protocol is enabled or disabled, run the command: `system node run -node <node_name> -command options cdpd.enable`

Use the `system health cluster-switch show` command to identify the switches that the cluster switch health monitor is monitoring.

### Parameters

**-device** <text> - Device Name

Specifies the device name of the switch that you want to monitor. Data ONTAP uses the device name of the switch to identify the SNMP agent with which it wants to communicate.

**-address** <IP Address> - IP Address

Specifies the IP address of switch's management interface.

**-snmp-version** {SNMPv1|SNMPv2c} - SNMP Version

Specifies the SNMP version that Data ONTAP uses to communicate with the switch. The default is SNMP v2c.

**-community** <text> - Community String

Specifies the community string for SNMPv2 authentication. The default is cshm1!.

---

**[-discovered {true|false}]** - Is Discovered

Specifies whether Data ONTAP automatically discovers information about the switch. When set to true, Data ONTAP discovers the switch and updates information about its configuration. When set to false, Data ONTAP does not discover the switch. The default value is true.

Use false when you manually enter information about a switch. This ensures that Data ONTAP does not overwrite the configuration when a new discovery takes place.

Data ONTAP monitors the switch whether the setting is true or false.

**-model {NX5010|NX5020|CAT2960|OTHER}** - Model Number

Specifies the model number of the switch. You should not set this parameter to OTHER. Data ONTAP does not monitor switches that match this value. Data ONTAP sets this parameter to OTHER if a switch that it automatically discovers is not supported for health monitoring.

**-type {cluster-network|management-network}** - Switch Network

Specifies the switch type.

## Examples

```
cluster1::> system health cluster-switch create -device SwitchA -ipaddress  
1.2.3.4 -snmpversion SNMPv2c -community public -discovered false -model NX5010 -  
type cluster
```

Creates a new switch configuration for a switch named SwitchA.

## See Also

system node run system health cluster-switch show

---

## system health cluster-switch delete

Delete information about a cluster switch or management switch

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

### Description

The `system health cluster-switch delete` command disables switch health monitoring for a cluster or management switch.

### Parameters

**-device <text>** - Device Name

Specifies the name of the switch.

### Examples

```
cluster1::*>system health cluster-switch delete -device SwitchA
```

Disables monitoring for the switch named SwitchA.

## system health cluster-switch modify

Modify information about a switch's configuration

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

### Description

The `system health cluster-switch modify` command modifies information about a cluster switch or management switch. The cluster switch health monitor uses this information to monitor the switch.

### Parameters

**-device <text>** - Device Name

Specifies the device name of switch that you want to monitor.



---

**[-address <IP Address>]** - IP Address

Specifies the IP address of switch's management interface.

**[-snmp-version {SNMPv1|SNMPv2c}]** - SNMP Version

Specifies the SNMP version that Data ONTAP uses to communicate with the switch. The default is SNMPv2c.

**[-community <text>]** - Community String

Specifies the community string for SNMPv2 authentication.

**[-discovered {true|false}]** - Is Discovered

Specifies whether Data ONTAP automatically discovers information about the switch. When set to true, Data ONTAP discovers the switch and updates information about its configuration. When set the false, Data ONTAP does not discover the switch. The default value is true.

Use false when you manually enter information about a switch. This ensures that Data ONTAP does not overwrite the configuration when a new discovery takes place.

Data ONTAP monitors the switch whether this setting is true or false.

**[-model {NX5010|NX5020|CAT2960|OTHER}]** - Model Number

Specifies the model number of the switch. You should not set this parameter to OTHER. Data ONTAP does not monitor switches that match this value. Data ONTAP sets this parameter to OTHER if a switch that it automatically discovers is not supported for health monitoring.

**[-type {cluster-network|management-network}]** - Switch Network

Specifies the switch type.

## Examples

```
cluster1::*> system health cluster-switch modify -device SwitchA -ipaddress 2.3.4.5
```

Modifies the IP address for the switch named SwitchA.

## system health cluster-switch show

Display the configuration for cluster and management switches

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

---

## Description

The `system health cluster-switch show` command displays configuration details for the monitored cluster switches and management switches.

## Parameters

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

Selects the fields that have the specified name.

| [-**snmp-config** ]

Displays the following information about a switch:

- Device Name
- Community String
- SNMP Version

| [-**instance** ] }

Selects detailed information for all the switches.

[-**device** <text>] - Device Name

Selects the switches that match the specified device name.

[-**address** <IP Address>] - IP Address

Selects the switches that match the specified IP address.

[-**snmp-version** {SNMPv1|SNMPv2c}] - SNMP Version

Selects the switches that match the specified SNMP version.

[-**community** <text>] - Community String

Selects the switches that match the specified community string.

[-**discovered** {true|false}] - Is Discovered

Selects the switches that match the specified discovery setting.

[-**model** {NX5010|NX5020|CAT2960|OTHER}] - Model Number

Selects the switches that match the specified model number.

[-**type** {cluster-network|management-network}] - Switch Network

Selects the switches that match the specified switch type.

---

**[-sw-version <text>]** - Software Version

Selects the switches that match the specified software version.

**Examples**

```
cluster1::>system health cluster-switch show
      Switch      Type      Address      Model      Software Version
-----
SwitchA      cluster  1.2.3.4      Nexus5010    Cisco IOS 4.1N1
```

The example above displays the configuration of all cluster switches and management switches.

```
cluster1::*>system health cluster-switch show -snmp-config
      Name      Community      SNMP Version
-----
SwitchA      public      SNMPv2c
```

The example above displays the community string, polling interval and SNMP version for all cluster switches and management switches.

**system health cluster-switch fan show**

Display fan information for cluster and management switches

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

**Description**

The `system health cluster-switch fan show` command displays the status of fans on the monitored switches.

**Parameters**

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

Selects the specified fields.

| **[-instance ]** }

Displays detailed information for all fans on all switches.

**[-device <text>]** - Switch Name

Selects the fans that belong to the specified switch.

---

**[-fan-name <text>]** - Fan or Fan Tray Name

Selects the fans that match the specified fan name or fan tray name.

**[-index <integer>]** - Sensor Index

Selects the fans that match the specified sensor index.

**[-fan-type {single|tray}]** - Single Fan or Fan Tray

Selects the fans that match the specified fan type.

**[-fan-status {operational|failed|not-operational|not-present|unknown}]** - Fan Status

Selects the fans that match the specified operational status.

**[-display-name <text>]** - Fan Display Name

Selects the fans that match the specified display name.

**[-unique-name <text>]** - Fan Unique Name

Selects the fan that matches the specified unique name.

**[-container-name <text>]** - Fan Container Name

Selects the fans that match the specified container name.

**[-is-psu-fan {yes|no}]** - Is Power Supply Unit Fan

Selects the fans that are PSU fans (*yes*) or are not PSU fans (*no*).

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Health Monitor

Selects the fans that the specified health monitor continuously monitors.

**[-error-description <text>]** - Error Description

Selects the fans that match the specified error description.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Resource Status

Selects the fans that match the specified status.

## Examples

```
cluster1::>system health cluster-switch fan show
```

Switch	Fan	Is FRU	Status	Container	Is PSU Fan	Error
SwitchA	PowerSupply	tray	operational			
	-1 Fan-1				unknown	no
SwitchA	FanModule-1	tray	not-present	FanBay-2	no	

---

The above example displays the fans and their status on the switch named SwitchA.

---

## system health cluster-switch interface show

Display interface information for cluster and management switches

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

### Description

The `system health cluster-switch interface show` command displays the status and configuration of network interfaces on the monitored switches.

### Parameters

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

Selects the fields that you specify.

| [-**counters** ]

Displays the current status of the following network counters:

- in-octets
- in-errors
- in-discards
- out-octets
- out-errors
- out-discards

| [-**instance** ] }

Displays detailed interface configuration for all monitored cluster switches

[-**device** <text>] - Switch Name

Selects the interface ports that belong to the specified switch.

[-**interface-name** <text>] - Interface Name

Selects the interface ports that match the specified interface name.

[-**index** <integer>] - Interface Index

Selects the interface ports that match the specified interface index.

---

**[-type <interface type>]** - Interface Type

Selects the interface ports that match the specified interface type.

**[-mtu <integer>]** - MTU

Selects the interface ports that match the specified maximum transfer unit.

**[-duplex-type {unknown|half-duplex|full-duplex}]** - Duplex Settings

Selects the interface ports that match the specified duplex setting.

**[-speed <integer>]** - Interface Speed(Mbps)

Selects the interface ports that match the specified interface speed in bits per second.

**[-admin-state {up|down|testing}]** - Administrative Status

Selects the interface ports that match the specified administrative status of the switch interface.

**[-oper-state {up|down|testing|unknown|dormant|not-present|lower-layer-down}]** - Operational Status

Selects the interface ports that match the specified operational status.

**[-is-isl {yes|no}]** - Is ISL

Selects the interface ports that are Inter-Switch links (yes) or are not Inter-Switch links (no).

**[-in-octets <Counter>]** - Input Octets

Selects the interface ports that match the specified number of octets entering the interface.

**[-in-errors <Counter>]** - Input Errors

Selects the interface ports that match the specified number of input packets that were dropped due to errors.

**[-in-discards <Counter>]** - Input Discards

Selects the interface ports that match the specified number of input packets that were silently discarded (possibly due to buffer overflow).

**[-out-octets <Counter>]** - Output Octets

Selects the interface ports that match the specified number of octets that exited the interface.

**[-out-errors <Counter>]** - Output Errors

---

Selects the interface ports that match the specified number of output packets that were dropped due to errors.

**[-out-discards <Counter>]** - Output Discards

Selects the interface ports that match the specified number of output packets that were silently discarded (possibly due to buffer overflow).

**[-interface-number <integer>]** - Interface Number

Selects the interface ports that match the specified interface number.

**[-unique-name <text>]** - Interface Unique Name

Selects the interface port that matches the specified unique name.

**[-display-name <text>]** - Interface Display Name

Selects the interface ports that match the specified display name.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Port Config Status

Selects the interface ports that match the specified status.

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Health Monitor

Selects the interface ports that the specified health monitor continuously monitors.

## Examples

```
cluster1::> system health cluster-switch interface show
Switch      Interface Number Index Type      Admin Status Operational Is-ISL MTU Duplex Speed
-----
SwitchA     FastEthernet0/1  1 10001 ethernetCsmacd up      down    no      1500 unknown 10
SwitchA     FastEthernet0/10 10 10010 ethernetCsmacd up      down    no      1500 unknown 10
```

The example above displays the interfaces on all cluster switches and management switches.

```
cluster1::>system health cluster-switch interface show -counters
Switch      Interface Octets In Errors In Discards In Octets Out Errors Out Discards
-----
cat2960-1   FastEthernet0/1  0      0      0      0      0      0      0
cat2960-1   FastEthernet0/10 0      0      0      0      0      0      0
```

The example above displays the counters on switch network interfaces for all the cluster switches and management switches.



---

## system health cluster-switch polling-interval modify

Modify the polling interval for monitoring cluster and management switch health

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

### Description

The `system health cluster-switch polling-interval modify` command modifies the interval in which the cluster switch health monitor polls cluster and management switches.

### Parameters

**[-polling-interval <integer>]** - Polling Interval

Specifies the interval in which the health monitor polls switches. The interval is in minutes. The default value is 5. The allowed range of values is 2 to 120.

### Examples

```
cluster1::> system health cluster-switch polling-interval modify -polling-interval 41
```

Modifies the polling interval of the switches.

## system health cluster-switch polling-interval show

Display the polling interval for monitoring cluster and management switch health

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

### Description

The `system health cluster-switch polling-interval show` command displays the polling interval used by the health monitor.

### Parameters

---

None

## Examples

```
cluster1::> system health cluster-switch polling-interval show
Polling Interval (in minutes): 40
```

The example above displays the polling interval period for the switches.

## system health cluster-switch power show

Display power information for cluster and management switches

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

### Description

The `system health cluster-switch power show` command displays the power supply status of the monitored cluster switches.

### Parameters

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

Selects the fields with the names that you specify.

| [-**instance** ] }

Displays detailed power supply information for all the switches.

[-**device** <text>] - Switch Name

Selects the PSUs that belong to the specified switch.

[-**psu-name** <text>] - Power Supply Name

Selects the PSUs that match the specified power supply name.

[-**oper-status** {operational|failed|not-operational|not-present|unknown}] - Operational Status

Selects the PSUs that match the specified operational status.

[-**error-description** <text>] - Error Description

Selects the PSUs that match the specified error description.

[-**display-name** <text>] - Power Supply Display Name

---

Selects the PSUs that match the specified display name.

**[-unique-name <text>]** - Power Supply Unique Name

Selects the PSU that matches the specified unique name.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Power Supply Resource Health

Selects the PSUs that match the specified status.

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Health Monitor

Selects the PSUs that match the specified monitor type.

**[-admin-status {on|off|not-defined|unknown}]** - Administrative Status

Selects the PSUs that match the specified administrative status for the power supply.

**Examples**

```
cluster1::> system health cluster-switch power show
Switch      Power Supply      Admin      Operational
-----      -
SwitchA     PowerSupply-1     on         operational
SwitchA     PowerSupply-2     on         operational
```

The example above displays the power-supply status for all cluster switches and management switches.

---

## system health cluster-switch temperature show

Display temperature information for cluster and management switches

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

### Description

The `system health cluster-switch temperature show` command displays the temperature status of switches monitored by the cluster switch health monitor.

### Parameters

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

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

| [-**instance** ] }

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

[-**device** <text>] - Switch Name

Selects the temperature sensors that belong to the specified switch.

[-**sensor-name** <text>] - Sensor Name

Selects the temperature sensors that match the specified temperature sensor name.

[-**index** <integer>] - Sensor Index

Selects the temperature sensors that match the specified sensor index.

[-**temperature** <integer>] - Temperature in Celsius

Selects the temperature sensors whose readings match the specified temperature value.

[-**threshold-severity** {Unknown|Other|Information|Degraded|Minor|Major|Critical|Fatal}, ...] - Threshold Severity

Selects the temperature sensors that match the specified threshold severity.

[-**threshold-value** <integer>, ...] - Threshold Value

Selects the temperature sensors that match the specified threshold value.

**[-sensor-status {normal|warning|alert|critical|not-present|not-operational|unknown}]** - Temperature Status

Selects the temperature sensors that match the specified operational status.

**[-display-name <text>]** - Sensor Display Name

Selects the temperature sensors that match the specified sensor display name.

**[-unique-name <text>]** - Sensor Unique Name

Selects the temperature sensor that matches the specified unique name.

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Health Monitor

Selects the temperature sensors that the specified health monitor continuously monitors.

**[-error-description <text>]** - Error Description

Selects the temperature sensors that match the specified fault error description.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Resource Status

Selects the temperature sensors that match the specified status.

## Examples

```
cluster1::> system health cluster-switch temperature show
Switch  Sensor              Reading  Threshold  Threshold  Status  Error
-----  -
SwitchA "Module-1, Intake-1"  24      Minor, Major  40, 50    normal
SwitchA "Module-1, Intake-2"  23      Minor, Major  40, 50    normal
```

The example above displays temperature status for all cluster switches and management switches.

---

## system health cluster-switch utilization show

Display cluster switch utilization

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

### Description

The `system health cluster-switch utilization show` command displays the CPU and memory utilization of switches monitored by the cluster switch health monitor.

### Parameters

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

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

| [-instance ] }

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

**[-device <text>]** - Switch Name

Selects the switches that match the specified switch name.

**[-cpu-busy-pct-5sec <integer>]** - CPU Busy Percent in Last 5 Seconds

Selects the switches that match the specified CPU busy percentage for the last 5 seconds.

**[-cpu-busy-pct-1min <integer>]** - CPU Busy Percent in Last 1 Minute

Selects the switches that match the specified CPU busy percentage for the last 1 minute.

**[-cpu-busy-pct-5min <integer>]** - CPU Busy Percent in Last 5 Minutes

Selects the switches that match the specified CPU busy percentage for the last 5 minutes.

**[-mem-free <integer>]** - Free System Memory in Kilobytes

Selects the switches that match the specified free system memory.

**[-mem-used <integer>]** - Used System Memory in Kilobytes

Selects the switches that match the specified used system memory.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - CPU health Status

Selects the switches that match the specified status.

**[-display-name <text>]** - Switch Display Name

Selects the switches that match the specified display name.

**[-unique-name <text>]** - Switch Unique Name

Selects the switch that matches the specified unique name.

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Health Monitor

Selects the switches that the specified health monitor continuously monitors.

**[-memory-utilization <integer>]** - Memory Utilization Percent

Selects the switches that match the specified percentage of memory utilization.

## Examples

```
cluster1::>system health cluster-switch utilization show
Switch      CPU Busy % CPU Busy % CPU Busy %      Free      Used      % Memory
              (5sec)  (1min)  (5min)  Memory(KB) Memory(KB) Utilized
-----
SwitchA          13          6          6          6757       16173       70
SwitchB          30          4          7       1117636       955772       46
SwitchC           8         10          6       1081920       991488       47
3 entries were displayed.
```

The example above displays the CPU utilization and memory consumption for all the cluster switches.

---

## system health config show

Display system health configuration

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

### Description

The `system health config show` command displays the configuration and status of each health monitor in the cluster. The command shows a health status for each health monitor. The health status is an aggregation of the subsystem health for each subsystem that the health monitor monitors. For example, if a health monitor monitors two subsystems and the health status of one subsystem is "ok" and the other is "degraded", the health status for the health monitor is "degraded".

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Use this parameter to list the health monitors present on the specified node.

[-monitor <hm\_type>] - Monitor

Use this parameter to display the health monitors with the specified monitor name.

[-subsystem <hm\_subsystem>, ...] - Subsystem

Selects the health monitors with the specified subsystems.

[-health {ok|ok-with-suppressed|degraded|unreachable|unknown}] - Health

Selects the health monitors with the specified health status.

[-mon-version <text>] - Monitor Version

Selects the health monitors with the specified monitor version.



---

**[-pol-version <text>]** - Policy File Version

Selects the health monitors with the specified health monitor policy version.

**[-context {Node |Cluster}]** - Context

Selects the health monitors with the specified running context.

**[-aggregator <hm\_type>]** - Aggregator

Selects the health monitors with the specified aggregator.

**[-resources <text>, ...]** - Resource

Selects the health monitors with the specified resource name.

**[-init-state {Invalid|Initailizing|Initialized|Starting\_Discovery|Starting\_Re-Discovery|Discovery\_Done\_Partially|Discovery\_Done}]** - Subsystem Initialization Status

Selects the health monitors with the specified subsystem initialization state.

**[-sub-pol-versions <text>]** - Subordinate Policy Versions

Selects the health monitors with the specified subordinate policy version.

## Examples

The example below displays information about health monitor configuration:

```
cluster1::> system health config show
Node      Monitor      Subsystem      Health
-----
node1     node-connect  SAS-connect    degraded
node1     system-connect SAS-connect    degraded
node1     system        SAS-connect    degraded
```

The example below displays detailed information about health monitor configuration:

```
cluster1::> system health config show -instance
Node: node1
Monitor: node-connect
Subsystem: SAS-connect
Health: degraded
Monitor Version: 1.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters
```

---

## system health node-connectivity adapter show

Show adapter resources and connectivity status

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

### Description

The `system health node-connectivity adapter show` command displays information about the adapters present on the different nodes in the cluster. By default, the command displays the following information about all adapters:

- Owner node name
- Adapter name
- Adapter is in use
- Adapter is enabled
- Number of shelves attached to the adapter
- Detailed status information

To display more details, use the `-instance` parameter.

### Parameters

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

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

| **[-instance ]** }

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

**[-node {<nodename>|local}]** - Node

Selects information about the shelves that the specified node owns.

**[-adapter-name <text>]** - Adapter Name

Selects information about the specified adapter name.

---

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Monitor Name

Selects information about the specified monitor name.

**[-wwn <text>]** - WWN

Selects information about the adapter with the specified Word Wide Node name.

**[-in-use {true|false}]** - In Use?

Selects information about the adapters currently in use.

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

Selects information about the adapters that are enabled.

**[-is-dual-attached {true|false}]** - Adapter Dual Attached

Selects information about the adapters that have dual attachments.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Status

Selects information about the adapters with the specified status.

**[-slot-num <integer>]** - Slot Number

Selects information about the adapters with the specified slot number.

**[-port-name <text>]** - Port Name

Selects information about the adapters with the specified port name.

**[-iom-port {Circle|Square}]** - IOM Port to be Connected to

Selects information about the adapters connected to the specified IOM port, either IOMA or IOMB.

**[-num-shelf <integer>]** - Number of Shelves

Selects information about the adapters with the specified number of shelves.

**[-shelf-list <text>, ...]** - List of Shelves

Selects information about the adapters with the specified shelf list.

**[-num-ioma <integer>]** - Number of Shelves Connected to IOMA

Selects information about the adapters with the specified number of shelves that are connected to IOMA.

**[-ioma-list <text>, ...]** - List of Shelves Connected to IOMA

Selects information about the adapters with the specified shelves that are connected to IOMA.

---

**[-num-iomb <integer>]** - Number of Shelves Connected to IOMB

Selects information about the adapters with the specified number of shelves that are connected to IOMB.

**[-iomb-list <text>, ...]** - List of Shelves Connected to IOMB

Selects information about the adapters with the specified shelves that are connected to IOMB.

**[-num-circle-port <integer>]** - Number of Shelves Connected to Circle port

Selects information about the adapters with the specified number of shelf circle ports.

**[-circle-port-list <text>, ...]** - List of Shelves Connected to Circle port

Selects information about the adapters with the specified list of shelves with circle ports connected.

**[-num-square-port <integer>]** - Number of Shelves Connected to Square port

Selects information about the adapters with the specified number of shelves with square ports connected.

**[-square-port-list <text>, ...]** - List of Shelves Connected to Square port

Selects information about all the adapters with the specified list of shelves with square ports connected.

## Examples

The following example displays information about all adapters for each node in the cluster:

```
cluster1::> system health node-connectivity adapter show
Node      Adapter Name  In Use?  Enabled  Number of Shelves  Status
-----
node1     1a            true     true      2                OK
node1     1b            false    false     0                OK
node1     1c            false    false     0                OK
node1     1d            true     true      2                OK
```

The following example displays detailed information about a specific adapter :

```
cluster1::> system health node-connectivity adapter show -adapter-name 1a -
instance
Node: node1
Adapter Name: 1a
Monitor Name: node-connect
WWN: 5:00e004:0000007:b8
In Use?: true
Is Enabled?: true
Adapter Dual Attached: true
Status: OK
Slot Number: 1
Port Name: a
IOM Port to be connected to: square
Number of Shelves: 2
List of Shelves: 50:05:0c:c1:02:00:0f:02,
```

---

```

Number of shelves connected to IOMA: 50:05:0c:c1:02:00:16:9d
List of shelves connected to IOMA: 50:05:0c:c1:02:00:0f:02,
50:05:0c:c1:02:00:16:9d
Number of shelves connected to IOMB: 0
List of shelves connected to IOMB: -
Number of shelves connected to Circle port: 0
List of shelves connected to Circle port: -
Number of shelves connected to Square port: 2
List of shelves connected to Square port: 50:05:0c:c1:02:00:0f:02,
50:05:0c:c1:02:00:16:9d

```

---

## system health node-connectivity disk show

Show disk resources and connectivity status

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

### Description

The `system health node-connectivity disk show` command displays information about disks. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all disks:

- Owner node name
- Disk name
- Disk bay number
- Number of paths to the disk
- Status

To display detailed information about disks, run the command with the `-instance` parameter

### Parameters

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

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

| **[-instance** ] }

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

**[-node** {<nodename>|local}] - Node

Selects information about all of the disks the node owns.

**[-serial-no** <text>] - Serial Number

Selects information about only the disk with the specified serial number.

---

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Monitor Name

Selects information about the disks with the specified monitor name.

**[-disk-name <text>]** - Disk Name

Selects information about the disk with the specified disk name.

**[-sec-name <text>]** - Secondary Disk Name

Selects information about the disk with the specified secondary disk name.

**[-uuid <text>]** - UUID

Selects information about the disk with the specified Universally Unique Identifier (UUID).

**[-shelf-id <integer>]** - Shelf ID

Selects information about the disks associated with the specified shelf ID.

**[-bay-no <integer>]** - Bay Number

Selects information about the disks with the specified bay number.

**[-num-paths <integer>]** - Number of Paths

Selects information about the disks with the specified number of paths.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Status

Selects information about the disks with the specified status.

## Examples

The example below displays information about all of the disks in the cluster:

```
cluster1::> system health node-connectivity disk show
```

Node	Disk Name	Bay	Paths	Status
node1	4d.31.2	2	2	OK
node1	4d.31.0	0	2	OK
node1	4d.31.1	1	2	OK
node1	4a.02.1	1	2	OK
node1	4a.02.2	2	2	OK
node1	4a.02.3	3	2	OK
node2	1d.31.2	2	2	OK
node2	1d.31.0	0	2	OK
node2	1d.31.1	1	2	OK
node2	1a.02.1	1	2	OK
node2	1a.02.2	2	2	OK
node2	1a.02.3	3	2	OK

The example below displays detailed information about a specific disk in the cluster:

```
cluster1::> system health node-connectivity disk show -disk-name 4d.31.2 -  
instance  
Node: node1
```

---

```
Serial Number: 3QP1G8SG000099433A81
Monitor Name: node-connect
Disk Name: 4d.31.2
Secondary disk Name: 4a.31.2
UUID:
5000C500:12BEC6A7:00000000:00000000:00000000:00000000:00000000:00000000
Shelf Id: 31
Bay Number: 2
Number of Paths: 2
Status: OK
```



---

## system health node-connectivity shelf show

Show shelf resources and connectivity status

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

### Description

The `system health node-connectivity shelf show` command displays information about shelves in the cluster. By default, the command displays the following information:

- Owner node name
- Shelf name
- Number of disks
- Number of paths to the shelf
- Status

To display detailed information about shelves, run the command with the `-instance` parameter

### Parameters

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

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

| **[-instance ]** }

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

**[-node** {<nodename>|local}] - Node

Selects information about the shelves that the node owns.

**[-uuid** <text>] - Shelf UUID

Selects information about the shelf with the specified UUID.

---

**[-monitor {node-connect|system-connect|system|controller|chassis|cluster-switch|example}]** - Monitor Name

Selects information about the shelves with the specified monitor name.

**[-shelf-name <text>]** - Shelf Name

Selects information about shelves with the specified shelf name.

**[-num-paths <integer>]** - Number of Paths

Selects information about shelves with the specified number of paths.

**[-num-disks <integer>]** - Number of Disks

Selects information about shelves with the specified number of disks

**[-ioma-adapter <text>]** - Adapter Connected to IOMA

Selects information about shelves with IOMA connected to the specified adapter.

**[-iomb-adapter <text>]** - Adapter Connected to IOMB

Selects information about shelves with IOMB connected to the specified adapter.

**[-ioma-adapter-slot <integer>]** - Slot number of Adapter Connected to IOMA

Selects information about shelves with IOMA connected to the specified adapter slot.

**[-iomb-adapter-slot <integer>]** - Slot number of Adapter Connected to IOMB

Selects information about shelves with IOMB connected to the specified adapter slot.

**[-ioma-adapter-port <text>]** - Port name of Adapter Connected to IOMA

Selects information about shelves with IOMA connected to the specified adapter port.

**[-iomb-adapter-port <text>]** - Port name of Adapter Connected to IOMB

Selects information about shelves with IOMB connected to the specified adapter port.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Status

Selects information about shelves with the specified status.

**[-id <integer>]** - Shelf ID

Selects information about the shelf with the specified shelf ID.

## Examples

The example below displays information about all shelves in the cluster:

```
cluster1::> system health node-connectivity shelf show
```

Num Num

---

Node	Shelf Name	Disks	Paths	Status
node1	4d.shelf2	4	2	OK
node1	4d.shelf31	3	2	OK
node2	1d.shelf2	4	2	OK
node2	1d.shelf31	3	2	OK

---

The example below displays detailed information about a specific shelf in the cluster:

```
cluster1:> system health node-connectivity shelf show -shelf-name 4d.shelf2 -
instance
```

```

Node: node1
Shelf UUID: 50:05:0c:c1:02:00:0f:02
Monitor Name: node-connect
Shelf name: 4d.shelf2
Number of Paths: 2
Number of Disks: 4
Adapter connected to IOMA: 4d
Adapter connected to IOMB: 4a
Slot number of Adapter connected to IOMA: 4
Slot number of Adapter connected to IOMB: 4
Port name of Adapter connected to IOMA: d
Port name of Adapter connected to IOMB: a
Status: OK
Shelf Id: 2
```

---

## system health policy definition modify

Modify system health policy definition

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

### Description

The `system health policy definition modify` enables or disables health monitoring policies based on input parameters the user provides.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node on which you want to enable or disable the policy.

**-monitor** <hm\_type> - Monitor

Use this parameter to specify the monitor name for which you want to be enable or disable the policy.

**-policy-id** <text> - Policy

Use this parameter to specify the policy identifier that you want to enable or disable.

**[-enable** {true|false}] - Policy Status

Use this parameter with the value "true" to enable the policy. Set the value to "false" to disable the policy.

**[-asup-enable** {true|false}] - Enable ASUP for this alert

Use this parameter to enable or disable an AutoSupport message for this alert.

### Examples

This example modifies policy state on the cluster:

```
cluster1::> system health policy definition modify -node node1  
-policy-id ControllerToShelfIomA_Policy -enable false -monitor *
```

## system health policy definition show

---

Display system health policy definitions

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

## Description

The `system health policy definition show` command lists the health monitor policy definitions as described by the health monitor policy file. The command displays the following fields:

- Node name
- Monitor name
- Policy name
- Policy rule expression
- Expression for joining two tables
- Policy status
- Alert identifier
- Number of alerts generated
- Previous alert time
- Responsible resource name

## Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects policy definitions for the specified node.

[-**monitor** <hm\_type>] - Monitor

Selects policy definitions with the specified monitor name.

---

**[-policy-id <text>]** - Policy

Selects policy definitions with the specified policy identifier.

**[-rule-expression <ArithExpr>]** - Rule Expression

Selects policy definitions with the specified rule of expression.

**[-where <ArithExpr>]** - Variable Equivalence

Selects rules that match the provided expression. This expression is part of the alert definition. It is shown for reference only and cannot be changed.

**[-enable {true|false}]** - Policy Status

Use this parameter with the value set to "true" to select policy definitions that are enabled. Set the value to "false" to select policy definitions that are disabled.

**[-alert-id <text>]** - Alert ID

Selects all policy definitions of the specified alert identifier.

**[-alert-count <integer>]** - Number of Alerts

Selects all policy definitions that caused alerts with the specified alert count.

**[-prev-alert-creation-time <MM/DD/YYYY HH:MM:SS>]** - Previous Alert Creation Time

Selects all policy definitions that caused the last alert at the specified alert time.

**[-responsible-resource-info <text>]** - Table and ID of Resource at Fault

Selects all policy definitions with the specified responsible resource.

**[-asup-enable {true|false}]** - Enable ASUP for this alert

Selects policy definitions for which AutoSupport messages are either enabled or disabled.

## Examples

The example below displays information about all the policy definitions present in the cluster:

```
cluster1::> system health policy definition show
Node      Monitor      Policy
-----
node1     node-connect      ControllerToShelfIomA_Policy
Policy Rule Expression: nschm_shelf_info.num-paths == 2 &&
                        nschm_shelf_info.iomb-adapter == NULL
                        Where: -
                        Enable: true
                        Alert ID: ControllerToShelfIomA_Alert
                        Number of Alerts: -
                        Previous Alert Time: -
                        Responsible Resource: nschm_shelf_info.name
```

---

The example below displays detailed information about all the policy definitions present in the cluster:

```
cluster1::> system health policy definition show -instance
Node: nodel
Monitor: node-connect
Policy: ControllerToShelfIomA_Policy
Rule Expression: nschm_shelf_info.num-paths == 2 &&
nschm_shelf_info.iomb-adapter == NULL
Variable Equivalence: -
Policy Status: true
Alert ID: ControllerToShelfIomA_Alert
Number of Alerts: -
Previous Alert Creation Time: -
Table and ID of Resource at Fault: nschm_shelf_info.name
```

---

## system health status show

Display system health monitoring status

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

### Description

The `system health status show` command displays the health monitor status. The possible states are:

- ok
- ok-with-suppressed
- degraded
- unreachable

### Parameters

None

### Examples

This example displays information about health monitoring status:

```
cluster1::> system health status show
      Status
-----
degraded
```

## system health subsystem show

Display the health of subsystems

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

### Description

The `system health subsystem show` command displays the health status of each subsystem for which health monitoring is available. This command aggregates subsystem health status from each node in the cluster. A subsystem's health status



---

changes to "degraded" when a health monitor raises an alert. You can use the `system health alert show` command to display information about generated alerts.

## Parameters

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

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

| [-instance ] }

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

**[-subsystem <hm\_subsystem>]** - Subsystem

Selects the specified subsystem.

**[-health {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Health

Selects subsystems that have the specified health status.

**[-init-state {Invalid|Initailizing|Initialized|Starting\_Discovery|Starting\_Re-Discovery|Discovery\_Done\_Partially|Discovery\_Done}]** - Initialization State

Selects subsystems that have the specified initialization state.

**[-outstanding-alert-count <integer>]** - Number of Outstanding Alerts

Selects subsystems that have the specified number of outstanding alerts.

**[-suppressed-alert-count <integer>]** - Number of Suppressed Alerts

Selects subsystems that have the specified number of suppressed alerts.

## Examples

The example below displays the health status of each subsystem:

```
cluster1::> system health subsystem show
Subsystem      Health
-----
SAS-connect    degraded
CIFS-NDO       OK
```

The example below displays detailed information about the health status of each subsystem:

```
cluster1::> system health subsystem show -instance
Subsystem: SAS-connect
Health: degraded
Initialization State: initialized
Number of Outstanding Alerts: 51
```

---

```
Number of Suppressed Alerts: 0
                          Subsystem: CIFS-NDO
                          Health: OK
                          Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
```

## See Also

system health alert show

---

## system health system-connectivity shelf show

Show shelf resources and connectivity status

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

### Description

The `system health system-connectivity shelf show` command displays the cluster level view of the shelves attached. The default command shows:

- Shelf UUID
- Shelf ID
- Connected nodes
- Number of paths to the shelf
- Status of the shelf

### Parameters

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

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

| [-**instance** ] }

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

[-**node** {<nodename>|local}] - Node

Selects the shelves that the specified node owns.

[-**uuid** <text>] - Shelf UUID

Selects the shelf with the specified Universal Unique Identifier.

[-**monitor** {node-connect|system-connect|system|controller|chassis|cluster-switch|example}] - Monitor Name

Selects the shelves with the specified monitor name.

[-**id** <integer>] - Shelf ID

Use this parameter to display the cluster view information about all the shelves with the specified shelf identifier.

**[-status {ok|ok-with-suppressed|degraded|unreachable|unknown}]** - Status

Selects the shelves with the specified status.

**[-num-paths <integer>]** - Number of Paths

Selects the shelves with the specified number of paths.

**[-connected-nodes <text>, ...]** - List of Nodes Connected to the Shelf

Selects the shelves with the specified connected nodes.

**[-num-nodes <integer>]** - Number of Nodes Connected to the Shelf

Selects the shelves with the specified number of nodes.

## Examples

The example below displays information about all the shelves in the cluster:

```
cluster1::> system health system-connectivity shelf show
Shelf UUID                               Shelf ID   Connected Nodes   Num Paths   Status
-----
50:05:0c:c1:02:00:0f:02                 2         node1, node2      4          OK
50:05:0c:c1:02:00:16:9d                 31        node1, node2      4          OK
```

The example below displays detailed information about all the shelves in the cluster:

```
cluster1::> system health system-connectivity shelf show -instance
Node: node1
Shelf UUID: 50:05:0c:c1:02:00:0f:02
Monitor Name: system-connect
Shelf ID: 2
Status: OK
Number of Paths: 4
List of Nodes Connected to the shelf: node1, node2
Number of Nodes Connected to the Shelf: 2

Node: node1
Shelf UUID: 50:05:0c:c1:02:00:16:9d
Monitor Name: system-connect
Shelf ID: 31
Status: OK
Number of Paths: 4
List of Nodes Connected to the shelf: node1, node2
Number of Nodes Connected to the Shelf: 2
```

---

## system license add

Add one or more licenses

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

### Description

This command adds a license to a cluster. To add a license you must specify a valid license key, which you can obtain from your sales representative.

### Parameters

{ **-license-code** <License Code> - License Code

This specifies the key of the license that is to be added to the cluster. For Data ONTAP 8.1, the parameter accepts a 14 digit upper-case alphanumeric character key. For Data ONTAP 8.2, the parameter accepts a list of 28 digit upper-case alphanumeric character keys.

| **-license-code** <License Code V2>, ... } - License Code V2

This specifies the key of the license that is to be added to the cluster. For Data ONTAP 8.1, the parameter accepts a 14 digit upper-case alphanumeric character key. For Data ONTAP 8.2, the parameter accepts a list of 28 digit upper-case alphanumeric character keys.

### Examples

The following Data ONTAP 8.2 example adds a list of licenses with the keys AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA and BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB to the cluster

```
cluster1::> system license add -license-code AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

The following Data ONTAP 8.1 example adds a license with the key AAAAAAAAAAAAAA to the cluster

```
cluster1::> system license add -license-code AAAAAAAAAAAAAA
```

## system license clean-up

---

Remove unnecessary licenses

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

## Description

This command manages licenses in the cluster that have no effect, and so can be removed. Licenses that have expired or are not affiliated with any controller in the cluster are deleted by this command.

## Parameters

**[-unused [true]]** - Remove unused licenses

If you use this parameter, the command removes licenses in the cluster that are not affiliated with any controller in the cluster.

**[-expired [true]]** - Remove expired licenses

If you use this parameter, the command removes licenses in the cluster that have expired.

**[-simulate | -n [true]]** - Simulate Only

If you use this parameter, the command will not remove the licenses. Instead it will display the licenses that will be removed if this parameter was not provided.

## Examples

The following example simulates and displays the licenses that can be cleaned up:

```
cluster1::> system license clean-up -n -unused -expired
Serial number: 1-80-000011
Owner: cluster1
Package                               Reason
-----
SnapLock                             Demo License has expired
SnapProtectApps                      Demo License has expired

Serial number: 1-81-00000000000000004062522917
Owner: none
Package                               Reason
-----
NFS                                   Serial number is not used by any node in the cluster
CIFS                                 Serial number is not used by any node in the cluster
```

The following example deletes the expired licenses:

```
cluster1::> system license clean-up -expired
2 demo licenses deleted.
```

The following example deletes the unused licenses:

```
cluster1::> system license clean-up -unused
```

---

2 unused licenses deleted.

## system license delete

Delete a license

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

### Description

This command deletes a license from a cluster.

### Parameters

{ **-feature** <Licensable Features> - Feature

Data ONTAP 8.1 only. This specifies the name of the feature license that is to be deleted from the cluster.

| [**-serial-number** <Node Serial Number>] - Serial Number

Data ONTAP 8.2 and above. This specifies the serial number of the license that is to be deleted from the cluster. If this parameter is not provided, the default value is the serial number of the cluster.

**-package** <Licensable Package> } - Package

Data ONTAP 8.2 and above. This specifies the name of the package that is to be deleted from the cluster.

### Examples

The following Data ONTAP 8.2 example deletes a license named CIFS and serial number 1-81-00000000000000000000123456 from the cluster:

```
cluster1::> system license delete -serial-number 1-81-00000000000000000000123456 -  
package CIFS
```

The following Data ONTAP 8.1 example deletes a license named CIFS from the cluster:

```
cluster1::> system license delete -feature CIFS
```

## system license show

Display licenses

---

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

## Description

This command displays the information about licenses in the system.

## Parameters

{ [-fields ]

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

| [-instance ] }

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

**[-serial-number <Node Serial Number>]** - Serial Number

Selects information about licenses that match the specified serial number.

**[-package <Licensable Package>]** - Package

Data ONTAP 8.2 and above. Selects license information about the specified package.

**[-owner <text>]** - Owner

Data ONTAP 8.2 and above. Selects license information about the packages that match the specified owner name.

**[-feature <Licensable Features>]** - Feature

Data ONTAP 8.1 only. Selects license information about the specified feature.

**[-serial-number <Cluster Serial Number>]** - Cluster serial Number

Selects information about licenses that match the specified serial number.

**[-limit <integer>]** - Limit

Data ONTAP 8.1 only. Selects information about the licenses that have the specified node count limit.

**[-expiration <MM/DD/YYYY HH:MM:SS>]** - Expiration Date

Data ONTAP 8.2 and above. Selects information about the licenses that have the specified expiration date.

**[-expiration-date <text>]** - Expiration Date



---

Data ONTAP 8.1 only. Selects information about licenses that have the specified expiration date.

**[-description <text>]** - Description

Selects information about licenses that match the specified description.

**[-type {license|site|demo}]** - Type

Data ONTAP 8.2 and above. Selects information about licenses that have the specified type.

**[-legacy {yes|no}]** - Legacy

Data ONTAP 8.2 and above. Selects information about licenses that match the specified legacy field.

**[-customer-id <text>]** - Customer ID

Data ONTAP 8.2 and above. Selects information about licenses that have the specified customer-id.

## Examples

The Data ONTAP 8.2 example below displays default information about all licensed packages in the cluster:

```
cluster1::> system license show
Serial Number: 1-80-123456
Owner: cluster1
Package      Type      Description      Expiration
-----
Base         site      Cluster Base License  -
iSCSI        site      iSCSI License      -
CDMI         site      CDMI License        -

Serial Number: 1-81-0000000000000001122334455
Owner: node1
Package      Type      Description      Expiration
-----
CDMI         license   CIFS License      -
SnapRestore  license   SnapRestore License  -
5 entries were displayed.
```

The Data ONTAP 8.1 example below displays default information about all licensed features in the cluster:

```
cluster1::> system license show
Feature      Cluster SN  Limit  Description
-----
Base         1-80-123456 666    Base License w/cluster size limit (nodes)
Mirror       1-80-123456 666    Mirror License
CIFS         1-80-123456 666    CIFS License
SnapRestore  1-80-123456 666    SnapRestore License
NFS          1-80-123456 666    NFS License
SnapMirror_DP 1-80-123456 666    SnapMirror Data Protection License
6 entries were displayed.
```

---

# system license status show

Display license status

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

## Description

This command displays the list of licensable packages in the system and their current licensing status.

## Parameters

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

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

| [-instance ] }

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

**[-package <Licensable Package>]** - Package Name

Selects information about the specified package.

**[-method <Licensed Method>]** - Licensed Method

Selects information about packages with the specified licensed method.

**[-expiration <MM/DD/YYYY HH:MM:SS>]** - Expiration Date

Selects information about licenses that have the specified expiration date.

## Examples

The example below displays the license status of the cluster:

```
cluster1::> system license status show
Package      Licensed Method  Expiration
-----
Base         site             -
NFS          none             -
CIFS         none             -
iSCSI        license          -
FCP          none             -
CDMI         none             -
SnapRestore  license          -
SnapMirror   license          -
```

---

FlexClone	none	-
SnapVault	none	-
SnapLock	none	-
SnapManagerSuite	license	-
SnapProtectApps	none	-
13 entries were displayed.		

---

## system node halt

Shut down a node

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

### Description

The `system node halt` command stops all activity on a node. You may supply a reason for the shutdown, which will be stored in the audit log. You may also keep partner nodes from performing storage takeover during the shutdown.

### Parameters

**-node** {<nodename>|local} - Node

Use this mandatory parameter to specify the node that you want to shut down. The value `local` specifies the current node.

**[-reason <text>]** - Reason for Shutdown

Use this parameter to enter a brief note to indicate the reason for the restart, which will be stored in the audit log. Providing this information assists support personnel with troubleshooting efforts.

**[-inhibit-takeover | -f [true]]** - Disallow Storage Takeover by Partner

This parameter optionally forces the shutdown and prevents storage failover.

Note:

If `-inhibit-takeover` is set to `true`, the default behavior as seen with command `storage failover show -fields onreboot` is ignored.

If you enter this command without using this parameter, its effective value is `false` and storage takeover is allowed. If you enter this parameter without a value, it is automatically set to `true` and storage takeover is disabled during reboot.

**[-dump | -d [true]]** - Create a Core Dump

If this parameter is set to `true`, it forces a dump of the kernel core when halting the node.

**[-skip-lif-migration [true]]** - Skip Migrating LIFs Away from Node

If this parameter is specified, LIF migration prior to the shutdown will be skipped. The default is to migrate LIFs prior to the shutdown. In the default case, the command

---

attempts to synchronously migrate data and cluster management LIFs away from the node prior to shutdown. If the migration fails or times out, the shutdown will be aborted.

## Examples

The following example shuts down the node named cluster1 for hardware maintenance:

```
cluster::> system halt -node cluster1 -reason 'hardware maintenance'
```

## See Also

storage failover show

---

## system node modify

Modify node attributes

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

### Description

The `system node modify` command sets the attributes of a node.

The owner, location, and asset tag attributes are informational only, and do not affect the operation of the node or the cluster. The cluster eligibility attribute marks a node as eligible to participate in a cluster. The epsilon attribute marks a node as the tie-breaker vote if the cluster has an even number of nodes.

Any field of type `<text>` may be set to any text value. However, if the value contains spaces or other special characters, you must enter it using double-quotes as shown in the example below.

Use the `system node show` command to display the field values that this command modifies.

### Parameters

**-node** {<nodename>|local} - Node

This mandatory parameter specifies which node will have its attributes modified. The value "local" specifies the current node.

**[-owner <text>]** - Owner

This optional text string identifies the node's owner. Fill it in as needed for your organization.

**[-location <text>]** - Location

Use this text string to identify the physical location of the node. This text string is optional; fill it in as needed for your organization.

**[-assettag <text>]** - Asset Tag

If your organization uses asset tags to track equipment, you can use this text string to store that tag's value.

**[-eligibility {true|false}]** - Eligibility

---

This parameter specifies whether the node is eligible to participate in a cluster. If you modify another node's eligibility to false, it will no longer be visible from other nodes in the cluster. If you modify the local node's eligibility to false, the node will no longer be active in the cluster and you will not be able to see any cluster nodes from it.

**[-epsilon {true|false}]** - Epsilon (privilege: advanced)

If specified as true for a node, this value designates the specified node as epsilon for this cluster. In a cluster, only one node can be designated as epsilon at any given time. A node can be designated as Epsilon to add weight to its voting in a cluster with an even number of nodes.

## Examples

The following example modifies the attributes of a node named node0. The node's owner is set to "IT" and its location to "Data Center 2."

```
node::> system node modify -node node0 -owner "IT" -location "Data Center 2"
```

## See Also

`system node show`

---

## system node reboot

Reboot a node

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

### Description

The `system node reboot` command restarts a node. You can supply a reason for the reboot, which is stored in the audit log. You can also keep partner nodes from performing storage takeover during the reboot and instruct the rebooted node to create a core dump.

### Parameters

**-node** {<nodename>|local} - Node

Specifies the node that is to be restarted. The value "local" specifies the current node.

**[-inhibit-takeover [true]]** - Disallow Storage Takeover by Partner

If set to `true`, this parameter specifies that the node's failover partner is not allowed to take over for the node when the node is rebooted. If you enter this command without using this parameter, its effective value is `false` and storage takeover is allowed. If you enter this parameter without a value, it is automatically set to `true` and storage takeover is disabled during reboot.

**[-reason <text>]** - Reason for Reboot

Use this parameter to enter a brief note to indicate the reason for the restart, which will be stored in the audit log. Providing this information assists support personnel with troubleshooting efforts.

**[-dump [true]]** - Create a Core Dump

If you would like the node to create a core dump before restarting, specify the `true` value with this parameter. If you enter this command without using this parameter, its effective value is `false` and the node doesn't create a core dump. If you enter this parameter without a value, it is automatically set to `true` and the node creates a core dump.

**[-skip-lif-migration [true]]** - Skip Migrating LIFs Away from Node

If this parameter is specified, LIF migration prior to the reboot will be skipped. The default is to migrate LIFs prior to the reboot. In the default case, the command attempts



---

to synchronously migrate data and cluster management LIFs away from the node prior to reboot. If the migration fails or times out, the reboot will be aborted.

## Examples

The command in the following example restarts the node named `cluster1` for a software upgrade:

```
cluster::> system node reboot -node cluster1 -reason "software upgrade"
```

## system node rename

Rename a node

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

## Description

The `system node rename` command changes a node's name. Both the node to be modified and the new name of that node must be specified with the following parameters. This command is best executed from the node that is being renamed, using the `-node local` parameter.

Use the `system node show` command to display the names of all the nodes in the current cluster.

## Parameters

**-node** {<nodename>|local} - Node

This parameter specifies which node you are renaming. The value `local` specifies the current node.

**-newname** <text> - New Name

Use this parameter to specify the new name of the node. The name of the node must begin with a letter and cannot be more than 47 characters long

## Examples

The following example changes the name of the node named `node3` to `node4`.

```
node::> system rename -node node3 -newname node4
```

## See Also

---

system node show

---

## system node revert-to

Revert a node to a previous release of Data ONTAP

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

### Description

The `system node revert-to` command reverts a node's cluster configuration to the given version. After the `system node revert-to` command has finished, the `revert_to` command must be run from the `nodeshell`. The `revert_to` command reverts the filesystem on individual nodes to the target release. Before running `revert-to` in the cluster shell, the target release must be installed on the node.

### Parameters

**-node** {<nodename>|local} - Node

Specifies the node that is to be reverted. The value `local` specifies the current node.

**-version** <revert version> - Data ONTAP Version

Specifies the version of Data ONTAP to which the node is to be reverted.

**[-check-only [true]]** - Capability Check

If set to `true`, this parameter specifies that the cluster configuration revert should perform checks to verify all of the preconditions necessary for `revert-to` to complete successfully. Setting the parameter to `true` does not run through the actual revert process. By default this option is set to `false`.

### Examples

The command in the following example reverts cluster configuration of a node named `node1` to version 8.1

```
cluster1::*>system node revert-to -node node1 -version 8.1
```

## system node run

Run interactive or non-interactive commands in the node shell

---

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

## Description

Use the `system node run` command to run certain commands from the nodeshell CLI on a specific node in the cluster. The nodeshell is the CLI that is available with 7-Mode deployments of Data ONTAP. You can run a single nodeshell command from the clustershell that returns immediately, or you can start an interactive nodeshell session from which you can run multiple nodeshell commands.

Nodeshell commands are useful for root-volume management and system troubleshooting. Commands that are available through the nodeshell are scoped to a single node in the cluster. That is, they affect only the node specified by the value of the `-node` parameter and do not operate on other nodes in the cluster. To see a list of available nodeshell commands, type '?' at the interactive nodeshell prompt. For more information on the meanings and usage of the available commands, use the `man` command in the nodeshell.

Only one interactive nodeshell session at a time can be run on a single node. Up to 24 concurrent, non-interactive sessions can be run at a time on a node.

When running the nodeshell interactively, exit the nodeshell and return to the clustershell by using the `exit` command. If the nodeshell does not respond to commands, terminate the nodeshell process and return to the clustershell by pressing Ctrl-D.

The `system node run` command is not available from the cluster-mode Web UI. The nodeshell can be invoked only from the Cluster-Mode CLI.

Note:

An alternate way to invoke the `system node run` command is by typing the `run` as a single word.

## Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node on which you wish to run the nodeshell command. If you specify only this parameter, the command starts an interactive nodeshell session that lasts indefinitely. You can exit the nodeshell to the clustershell by pressing Ctrl-D or by typing the `exit` command.

{ [-**command** <text>, ...] - Command to Run

---

This optionally specifies the name of a single nodeshell command to run on the specified node. To see a list of available nodeshell commands, type '?' at an interactive nodeshell prompt.

| [-reset [true]] } - Reset Existing Connection

If this parameter is specified with the `true` value, it terminates any existing interactive nodeshell session on the specified node. The default value is `false`.

## Examples

The following example runs the nodeshell command `sysconfig -V` on a node named `node1`:

```
cluster1::> system node run -node node1 -command sysconfig -V
volume node1_aggr0 (1 RAID group):
    group 0: 3 disks
```

The following example starts a nodeshell session on a node named `node2` and then runs the nodeshell `sysconfig -V` command. The system remains in the nodeshell after running the `sysconfig -V` command.

```
cluster1::> run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI
node2> sysconfig -V
volume node2_aggr0 (1 RAID group):
    group 0: 3 disks
node2>
```

The following example starts a nodeshell session on a node named `node1` and then runs two nodeshell commands, `aggr status` first and `vol status` second. Use quotation marks and semicolons when executing multiple nodeshell commands with a single `run` command.

```
cluster1::> run -node node1 -command "aggr status; vol status"
    Aggr State      Status      Options
    aggr0 online    raid_dp, aggr    root
                    parity uninit'd!
                    32-bit
    aggr1 online    raid_dp, aggr
                    parity uninit'd!
                    32-bit
    Volume State    Status      Options
    vol0 online    raid_dp, flex  root, nvfail=on
                    parity uninit'd!
    root_vs0 online raid_dp, flex  create_ucose=on,
                    cluster      convert_ucose=on,
                    parity uninit'd! maxdirsiz=102400
```

---

## system node show

Display the list of nodes in the cluster

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

### Description

The `system node show` command displays information about the nodes in a cluster. You can limit the display to specific types of information and specific nodes, or you can filter the display by specific field values.

To list the values in use for a particular field, include the `-fields` parameter. Use the `system node modify` command to change some of the field values that this command displays.

### Parameters

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

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

| **[-inventory]**

Displays inventory information such as serial numbers, asset tags, system identifiers, and model numbers.

| **[-messages]**

Displays system messages for each node.

| **[-instance]** }

Displays detailed information about each node.

**[-node** {<nodename>|local}] - Node

Selects the name of a node for which information is to be displayed. If this parameter is not specified, the command displays information about all nodes in the cluster.

**[-owner** <text>] - Owner

Selects information about nodes with the specified owner value.

**[-location** <text>] - Location

---

Selects information about nodes at the specified physical location.

**[-model <text>]** - Model

Selects information about nodes that have the specified model number.

**[-serialnumber <text>]** - Serial Number

Selects information about the node that has the specified serial number.

**[-assettag <text>]** - Asset Tag

Selects information about the node that has the specified asset tag value.

**[-uptime <timeticks>]** - Uptime

Selects information about nodes with the specified uptime characteristics. The time value format is "D days HH:MM", enclosed in double-quotes. This parameter is most useful when used with a range indicator such as less than or greater than, as in `show - uptime >"30 days 00:00"`.

**[-nvramid <nvramid>]** - NVRAM System ID

Selects information about the node with the specified NVRAM system ID.

**[-systemid <text>]** - System ID

Selects information about the node that has the specified system ID.

**[-vendor <text>]** - Vendor

Selects information about nodes from the specified vendor.

**[-health {true|false}]** - Health

Selects information about nodes that have the specified health value. Specify `true` to select healthy nodes, and `false` to select unhealthy nodes.

**[-eligibility {true|false}]** - Eligibility

Selects information about nodes that are eligible or ineligible to participate in a cluster. Note that, from the cluster shell prompt you can only perform this command on members of the current cluster.

**[-epsilon {true|false}]** - Epsilon (privilege: advanced)

Selects information about nodes that have the specified Epsilon setting. In a cluster, only one node can be designated as Epsilon at any given time. A node can be designated as Epsilon to add weight to its voting in a cluster with an even number of nodes. This is useful to find out which node, if any, in the current cluster has been designated as Epsilon.

---

## Examples

The example below displays information about all nodes in the cluster:

```
node::> system node show
Node      Health Eligibility Uptime      Model      Owner      Location
-----
node0     true     true      89 days 23:47 MODELXX    IT         Data Center 2
node1     true     true      15 days 22:37 MODELXX              Data Center 2
node2     true     true      15 days 23:00 MODELXX              Data Center 2
node3     true     true      15 days 22:37 MODELXX              Data Center 2
4 entries were displayed.
```

The example below displays the locations and model numbers of all nodes that are in physical locations that have names beginning with "Lab":

```
node::> system node show -location lab* -fields location, model
node      location model
-----
node5     Lab 1    MODELXX
node7     Lab 3    MODELXX
node9     Lab 5    MODELXX
```

## See Also

`system node modify`



---

## system node systemshell

Access diagnostic shell

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

### Description

The `system node systemshell` command invokes a low-level command shell for diagnostic and troubleshooting purposes. This command is available only at the advanced privilege level and higher.

Attention:

The systemshell is not intended for general administrative purposes. Use it only with guidance from technical support. Misuse of the systemshell can result in system failure and data loss or data corruption.

Log into the systemshell only with the predefined `diag` user account. You must set the initial password for the `diag` account using the `security login password` command.

Commands that are available through the systemshell are "scoped" to a single node in the cluster. That is, they affect only the node specified by the value of the `-node` parameter and do not operate on other nodes in the cluster.

To exit from the systemshell and return to the clustershell, use the `exit` command or press Ctrl-D.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the name of the node on which you wish to run the systemshell. If you specify only this parameter, the command switches your session to the systemshell indefinitely. You can exit the systemshell to the clustershell by pressing Ctrl-D or by typing the `exit` or `logout` commands.

### Examples

The following example starts and then exits the systemshell on a node named `node1`.

```
node::*> system node systemshell -node node1
Type 'exit' or 'Ctrl-D' to return to the CLI
```

---

```
Data ONTAP/amd64 (node1) (ttypl)
login: diag
Password:
Last login: Fri Nov  7 19:09:58 from localhost

%exit
logout
node::*>
```

## See Also

security login password exit

---

## system node autosupport invoke

Generate and send an AutoSupport message

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

### Description

The `system node autosupport invoke` command sends an AutoSupport message from a node.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node from which the AutoSupport message is sent.

**[-message <text>]** - Message Text to Include

Use this parameter to specify text sent in the subject line of the AutoSupport message. This parameter is not available when the `-type` parameter is set to performance.

**-type** {test|performance|all} - Type of AutoSupport Collection to Issue

Use this parameter to specify the type of AutoSupport collection to issue. There is no default; you must specify a `-type`.

- **test** - The message contains basic information about the node. When the AutoSupport message is received by technical support, an e-mail confirmation is sent to the system owner of record. This enables you to confirm that the message is being received by technical support.
- **all** - The message contains all collected information about the node.
- **performance** - The message contains only performance information about the node. This parameter has effect only if performance AutoSupport messages are enabled, which is controlled by the `-perf` parameter of the `system node autosupport modify` command.

**[-uri <text>]** - Alternate Destination for this AutoSupport

Use this parameter to send the AutoSupport message to the destination you specify instead of the configured destination. Only "file", "mailto", "http", and "https" protocols are supported. If this parameter is omitted, the message is sent to the all of the recipients defined by the `system node autosupport modify` command.

---

**[-force [true]]** - Generate and Send Even if Disabled

Use this parameter to generate and send the message even if AutoSupport is disabled on the node.

## Examples

The following example sends a test AutoSupport message from a node named node0 with the text "Testing ASUP":

```
cluster1::> system node autosupport invoke -node node0 -type test -message  
"Testing ASUP"
```

## See Also

system node autosupport modify

---

## system node autosupport modify

Modify AutoSupport configuration

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

### Description

The `system node autosupport modify` command modifies the AutoSupport configuration of a node.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node being configured.

**[-state** {enable|disable}] - State

Use this parameter to specify whether AutoSupport is enabled or disabled on the node. The default setting is `enable`. When AutoSupport is disabled, messages are not sent to anyone, including the vendor's technical support, your internal support organization, or partners.

**[-mail-hosts** <text>, ...] - SMTP Mail Hosts

Use this parameter to specify up to five SMTP mail hosts through which the node sends AutoSupport messages. This parameter is required if you specify e-mail addresses in the `-to`, `-noteto`, or `-partner-address` parameters or if you specify `smtp` in the `-transport` parameter. Separate multiple mail hosts with commas with no spaces in between. The AutoSupport delivery engine will attempt to use these hosts for delivery in the order you specify them. One can optionally specify a username/password for authentication with the `mailserver(rfc4954)`. The format of the username password is `user1:pw1@mailhost1`. Username/password may be specified on `none`, `all`, or `some` of the mailhosts. The default is `mailhost`.

**[-from** <mail address>] - From Address

Use this parameter to specify the e-mail address from which the node sends AutoSupport messages. The default is `Postmaster@xxx` where `xxx` is the name of the system.

**[-to** <mail address>, ...] - List of To Addresses

---

Use this parameter to specify up to five e-mail addresses to receive AutoSupport messages that are most relevant for your internal organization. Separate multiple addresses with commas with no spaces in between. For this parameter to have effect, the `-mail-hosts` parameter must be configured correctly. Individual trigger events can change the default usage of this parameter using the `-to` parameter of the `system node autosupport trigger modify` command. By default, no list is defined.

**`[-noteto <mail address>, ...]`** - List of Noteto Addresses

Use this parameter to specify up to five addresses to receive a short-note version of AutoSupport messages that are most relevant for your internal organization. Short-note e-mails contain only the subject line of the AutoSupport message, which is easier to view on a mobile device. For this parameter to have effect, the `-mail-hosts` parameter must be configured correctly. Individual trigger events can change the default usage of this parameter using the `-noteto` parameter of the `system node autosupport trigger modify` command. By default, no list is defined.

**`[-partner-address <mail address>, ...]`** - List of Partner Addresses

Use this parameter to specify up to five e-mail addresses to receive all AutoSupport messages including periodic messages. This parameter is typically used for support partners. For this parameter to have effect, the `-mail-hosts` parameter must be configured correctly. By default, no list is defined.

**`[-support {enable|disable}]`** - Send AutoSupport Messages to Vendor Support

Use this parameter to specify whether to send all AutoSupport messages to your vendor's technical support. (Destination information is pre-defined and does not require configuration.) When `-state` is enabled and `-support` is disabled, messages are sent to the addresses specified in the `-to`, `-noteto`, or `-partner-address` parameters but are not sent to your vendor's technical support. The default is `enable`.

**`[-transport {smtp|http|https}]`** - Protocol to Contact Support

Use this parameter to specify the protocol used to deliver AutoSupport messages to your vendor's technical support. This parameter applies only when the `-support` parameter is set to `enable`. If you specify `http` or `https` and your network uses a proxy, you must also set the `-proxy-url` parameter. If you specify `smtp`, you must also configure the `-mail-hosts` parameter.

**`[-proxy-url <text>]`** - Support Proxy URL

Use this parameter to specify an HTTP or HTTPS proxy if the `-transport` parameter is set to `HTTP` or `HTTPS` and your organization uses a proxy. Enter the URL without an `http://` or `https://` prefix. If authentication is required, use the format `"[username]:[password]@[host][:[port]]"`. The default is an empty string.

**`[-hostname-subj {true|false}]`** - Hostname Subject

---

Use this parameter to specify whether the hostname of the node is included in the subject line of the AutoSupport message. The default is `false`. This parameter applies only if the `-remove-private-data` parameter is `true`.

**`[-nht {true|false}]`** - NHT Enable

Use this parameter to specify whether NHT disk drive health data is sent to technical support and addresses specified in the `-partner-address` parameter when disk drives fail. The default is `true`.

**`[-perf {true|false}]`** - Performance Data Enable

Use this parameter to specify whether performance data is sent to technical support and addresses specified in the `-partner-address` parameter. The default is `true`.

**`[-retry-interval <[<integer>h][<integer>m][<integer>s]>]`** - Retry Interval

Use this parameter to specify the amount of time to delay before trying to send an AutoSupport message again after a sending failure. Values may end with "s", "m", or "h" to indicate seconds, minutes, or hours, respectively. The minimum interval is 30 seconds and the maximum is 1 day. The default is 4 minutes.

**`[-retry-count <integer>]`** - Retry Count

Use this parameter to specify the number of times to try resending mail before dropping it. The minimum number is 5 and the maximum is 4,294,967,294. The default is 15 times.

**`[-reminder {true|false}]`** - Reminder Enable

Use this parameter to enable or disable a reminder message that is sent when AutoSupport is not configured to send messages to technical support. This reminder is logged as an EMS event called "autosupport.general.reminder" every 24 hours. The default is `true`.

**`[-periodic-tx-window <[<integer>h][<integer>m][<integer>s]>]`** - The Transmission Window

Use this parameter to specify a randomized delay window for periodic AutoSupport messages. The transmission window prevents message floods from periodic AutoSupport triggers such as "callhome.weekly", "callhome.performance.data", "callhome.nht.data", and "callhome.management.log". Valid values range from 0 minutes to 240 minutes (4 hours). The default is 60 minutes (1 hour). Setting the value to 0 disables the randomized delay.

**`[-max-http-size {<integer>[KB|MB|GB|TB|PB]}]`** - Maximum HTTP Size

Use this parameter to specify the maximum file size (in bytes by default, but can also be specified in KB, MB, TB or PB) for HTTP and HTTPS transfers. This parameter applies only to messages sent to technical support and only if the `-transport` parameter is set to

---

HTTP or HTTPS. Setting the value to 0 disables the delivery size budget. The default is 10 MB.

If the size of the AutoSupport message exceeds this value, AutoSupport will deliver as much of the message as possible. You can use the "system node autosupport manifest show" command to identify the sections of the message that AutoSupport sent. AutoSupport collects and sends the content in order of priority. The priority is predefined for each AutoSupport message. To identify the collection order for an AutoSupport trigger, use the "system node autosupport trigger show" command with the -instance parameter.

**[-max-smtp-size <integer>[KB|MB|GB|TB|PB]]** - Maximum SMTP Size

Use this parameter to specify the maximum file size (in bytes by default, but can also be specified in KB, MB, TB or PB) for SMTP (e-mail) transfers. This parameter applies to messages sent to the addresses specified in the -to, -noteto, and -partner-address parameters. If the -transport parameter is set to smtp, this parameter also applies to messages sent to the vendor's technical support. Setting the value to 0 disables the delivery size budget. The default is 5 MB.

If the size of the AutoSupport message exceeds this value, AutoSupport will deliver as much of the message as possible. You can use the "system node autosupport manifest show" command to identify the sections of the message that AutoSupport sent. AutoSupport collects and sends the content in order of priority. The priority is predefined for each AutoSupport message. To identify the collection order for an AutoSupport trigger, use the "system node autosupport trigger show" command with the -instance parameter.

**[-remove-private-data {true|false}]** - Remove Sensitive Data

Use this parameter with the value `true` to remove, encode, or mask sensitive data from AutoSupport attachments and headers. Use this feature to eliminate private data from all AutoSupport messages.

Eliminated data might include: IP addresses, MAC addresses, URIs, DNS names, e-mail addresses, port numbers, node names, Vserver names, cluster names, aggregate names, volume names, junction paths, policy names, user IDs, group IDs, LUNs, and qtree names.

The default is `false`.

Note:

Changing this value from false to true deletes the AutoSupport history and all files associated with it.

**[-validate-digital-certificate {true|false}]** - Validate Digital Certificate Received



---

Use this parameter with the value `true` to force the node to validate digital certificates that it receives. The default is `true`

**[-local-collection {true|false}]** - Continue Local Collection while Disabled

Use this parameter with the value `false` to disable local storage of AutoSupport files when sending of AutoSupport messages is disabled. The default is `true`, which causes the node to store AutoSupport files locally even if AutoSupport is disabled.

To enable or disable sending of AutoSupport messages, use the `-state` parameter.

Note:

If local collection is `false`, valuable historical information will not be available to technical support staff to quickly solve future problems.

## Examples

The following example enables AutoSupport on a node named `node3` with the following settings:

- SMTP mail host named `smtp.example.com`.
- E-mail "from" address of `alerts@node3.example.com`
- E-mail "to" address of `support@example.com`
- AutoSupport messages sent to support personnel
- HTTPS set as transport protocol
- Short-note address of `pda@example.com`
- If sending fails, the system will wait 23 minutes before retrying.

```
cluster1::> system node autosupport modify -node node3 -state enable -mail-hosts
smtp.example.com -from alerts@node3.example.com -to support@example.com -support
enable -transport https -noteto pda@example.com -retry-interval 23m
```

The following examples show how to modify AutoSupport URLs when using IPv6 address literals:

```
cluster1::> system node autosupport modify -node node1 -mail-hosts
[2620:10a:4002:6004::bbbb]:25
cluster1::> system node autosupport modify -node node1 -proxy-url
username:password@[2620:10a:4002:6004::bbbb]:8080
```

## See Also

`system node autosupport trigger modify` `event show-suppression`

---

## system node autosupport show

Display AutoSupport configuration

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

### Description

The `system node autosupport show` command displays the AutoSupport configuration of one or more nodes.

### Parameters

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

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

| [-config ]

Use this parameter to display the retry interval, retry count, throttle, and reminder settings of all nodes in the cluster.

| [-nht-performance ]

Selects NHT and performance information about all nodes in the cluster.

| [-recent ]

Selects the subject and time of the last AutoSupport message generated by each node in the cluster.

| [-support-http ]

Displays for each node in the cluster whether HTTP support is enabled for each node in the cluster, and identify the transport protocol and the support proxy URL used by each node.

| [-support-smtp ]

Displays for each node in the cluster whether SMTP (e-mail) support is enabled for each node in the cluster, and identify the transport protocol and the "to" mail address used by each node.

| [-instance ] }

---

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

**[-node {<nodename>|local}]** - Node

Displays detailed information about the node you specify.

**[-state {enable|disable}]** - State

Selects information only about nodes that have the AutoSupport state you specify.

**[-mail-hosts <text>, ...]** - SMTP Mail Hosts

Selects information only about nodes that use the mail hosts you specify.

**[-from <mail address>]** - From Address

Selects information only about nodes that have the "from" e-mail address you specify.

**[-to <mail address>, ...]** - List of To Addresses

Selects information only about nodes that have the "to" e-mail addresses you specify.

**[-noteto <mail address>, ...]** - List of Noteto Addresses

Selects information about nodes that send short-note e-mail messages to the e-mail addresses you specify. Short-note e-mails contain only the subject line of the AutoSupport message, which is easier to view on a mobile device.

**[-partner-address <mail address>, ...]** - List of Partner Addresses

Selects information only about nodes that have the "partner-address" e-mail addresses you specify. These addresses are not subject to the delivery limitations configured for the "-to" addresses of AutoSupport triggers.

**[-support {enable|disable}]** - Send AutoSupport Messages to Vendor Support

Use this parameter with the value "enable" to select information about nodes that send AutoSupport messages to your vendor's technical support. Use "disable" to select information about nodes that do not send these AutoSupport messages.

**[-transport {smtp|http|https}]** - Protocol to Contact Support

Selects information about nodes that use the specified protocol to send AutoSupport messages.

**[-proxy-url <text>]** - Support Proxy URL

Selects information only about nodes that use the proxy URL you specify.

**[-hostname-subj {true|false}]** - Hostname Subject

---

Selects information about nodes that include their hostname in the "Subject:" line of AutoSupport messages. If the parameter "remove-private-data" is `false`, this parameter has no effect.

**[-nht {true|false}]** - NHT Enable

Use this parameter with the value "true" to select information about nodes that send NHT disk drive data. Use "false" to select information about nodes that do not send NHT data.

**[-perf {true|false}]** - Performance Data Enable

Use this parameter with the value "true" to select information about nodes that send periodic performance AutoSupport messages. Use "false" to select information about nodes that do not send periodic performance messages.

**[-retry-interval <[<integer>h][<integer>m][<integer>s]>]** - Retry Interval

Selects information about nodes that use the retry interval you specify.

**[-retry-count <integer>]** - Retry Count

Selects information about nodes that use the retry count you specify.

**[-reminder {true|false}]** - Reminder Enable

Use this parameter with the value "true" to select information about nodes that send messages reminding administrators to enable AutoSupport. Use "false" to select information about nodes that do not send reminder messages.

**[-periodic-tx-window <[<integer>h][<integer>m][<integer>s]>]** - The Transmission Window

Selects information only about nodes that have a transmission window with the time interval you specify. The transmission window prevents message floods from periodic AutoSupport triggers such as "callhome.weekly", "callhome.performance.data", "callhome.nht.data", and "callhome.management.log".

**[-last-subject <text>]** - Last Subject Sent

Selects information only about nodes whose last AutoSupport message had the "Subject:" line you specify.

**[-last-time <MM/DD/YYYY HH:MM:SS>]** - Last Time Sent

Selects information about nodes whose last AutoSupport message was sent at the specified date and time.

**[-max-http-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum HTTP Size

---

Selects information about nodes that limit the maximum size of HTTP transfers to the file size you specify.

**[-max-smtp-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum SMTP Size

Selects information only about nodes that limit the maximum size of SMTP (e-mail) transfers to the file size you specify.

**[-remove-private-data {true|false}]** - Remove Sensitive Data

Use this parameter with the value "true" to select information about nodes that remove sensitive data from AutoSupport messages. Use "false" to select information about nodes that do not remove sensitive data.

**[-validate-digital-certificate {true|false}]** - Validate Digital Certificate Received

Use this parameter with the value "true" to select information about nodes that validate digital certificates they receive. Use this parameter with the value "false" to select information about nodes that do not validate digital certificates.

**[-local-collection {true|false}]** - Continue Local Collection while Disabled

Use this parameter with the value "true" to select information about nodes that collect AutoSupport files locally if AutoSupport is disabled. Use "false" to display information about nodes that do not collect AutoSupport files locally if AutoSupport is disabled.

## Examples

The example below displays the AutoSupport configuration for a node named node3:

```
cluster1::> system node autosupport show -node node3
Node: node3
State: enable
SMTP Mail Hosts: smtp.example.com
From Address: alerts@node3.example.com
List of To Addresses: support@example.com
List of Neteto Addresses: -
List of Partner Addresses: partner@node4.example.com
Send AutoSupport Messages to Vendor Support: enable
Protocol to Contact Support: https
Support Proxy URL: support.proxy.example.com
Hostname Subject: true
NHT Enable: true
Performance Data Enable: true
Retry Interval: 4m
Retry Count: 15
Reminder Enable: true
The Transmission Window: 1h
Last Subject Sent: WEEKLY
Last Time Sent: 3/11/2011 06:00:03
Maximum HTTP Size: 10MB
Maximum SMTP Size: 5MB
Remove Sensitive Data: false
Validate Digital Certificate Received: true
Continue Local Collection while Disabled: true
```

## See Also

---

event show-suppression   system node autosupport trigger show  
system node autosupport budget show   system node autosupport history show  
system node autosupport manifest show

---

## system node autosupport destinations show

Display a summary of the current AutoSupport destinations

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

### Description

The `system node autosupport destinations show` command displays a list of all message destinations used by AutoSupport. The command provides you with a quick summary of all addresses and URLs that receive AutoSupport messages from all nodes in the cluster.

### Parameters

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

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

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Selects destinations that receive AutoSupport messages from the node you specify.

[-destinations <text>, ...] - Destinations

Selects destination lists for nodes that send AutoSupport messages to the destinations you specify.

### Examples

The example below displays all of the destinations in use by the current cluster. Each node uses the same destination for HTTP POST, HTTP PUT, and e-mail notifications.

```
cluster1::> system node autosupport destinations show
Node
  Destinations
-----
node1
  https://asuppost.example.com/cgi-bin/asup.cgi
  https://asupput.example.com/cgi-bin/asup.cgi
  support@example.com
node2
```

---

```
https://asuppost.example.com/cgi-bin/asup.cgi  
https://asupput.example.com/cgi-bin/asup.cgi  
support@example.com
```



---

## system node autosupport history retransmit

Selectively retransmit a previously collected AutoSupport.

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

### Description

The `system node autosupport history retransmit` command retransmits a locally stored AutoSupport message.

Support personnel might ask you to run this command to retransmit an AutoSupport message. You might also retransmit an AutoSupport message if you run the `system node autosupport history show` command and notice that a message was not delivered.

If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.

Use the `system node autosupport history show` command to display the 50 most recent AutoSupport messages, which are available for retransmission.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node from which the AutoSupport message is sent.

**-seq-num** <Sequence Number> - AutoSupport Sequence Number

Use this parameter to specify the sequence number of the AutoSupport message to retransmit.

**-uri** <text> - Destination to Send this AutoSupport

Use this parameter to specify the HTTP, HTTPS, FILE, or MAILTO uniform resource indicator (URI) to which the AutoSupport message is sent.

**[-size-limit** {<integer>[KB|MB|GB|TB|PB]] - Transmit Size Limit for this AutoSupport.

Use this parameter to specify a size limit for the retransmitted AutoSupport message. If the message information exceeds this limit, it will be trimmed to fit the limit you specify.

---

Omit the size limit or set it to 0 to disable it, which is useful to retransmit an AutoSupport message that was truncated by a mail or Web server due to the default size limits.

## Examples

The following example retransmits the AutoSupport message with sequence number 45 on the node "node1" to a support address by e-mail.

```
cluster1::> system node autosupport history retransmit -node node1 -seq-num 45 -  
uri mailto:support@example.com
```

## See Also

`system node autosupport history show`

---

## system node autosupport history show

Display recent AutoSupport messages

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

### Description

The `system node autosupport history show` command displays information about the 50 most recent AutoSupport messages sent by nodes in the cluster. By default, it displays the following information:

- AutoSupport sequence number
- Destination type, such as smtp
- Status of delivery, such as sent-successful
- Attempt count
- Time of last update

### Parameters

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

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

| [-**delivery** ]

Displays destination information about each AutoSupport message.

| [-**detail** ]

Displays trigger and subject information about each AutoSupport message.

| [-**instance** ] }

Displays the following additional information:

- Trigger event
- Subject of the message
- Delivery URI

- 
- Last error

**[-node {<nodename>|local}]** - Node

Selects AutoSupport messages sent from the node you specify.

**[-seq-num <Sequence Number>]** - AutoSupport Sequence Number

Selects AutoSupport messages with the sequence number you specify. Sequence numbers are unique to a node. Add the `-node` parameter to display information about an individual message.

**[-destination {smtp|http|noteto|retransmit}]** - Destination for this AutoSupport

Selects AutoSupport messages that were sent to the destination type you specify.

**[-trigger <Message Name>]** - Trigger Event

Selects AutoSupport messages that match the trigger event you specify.

**[-last-update <MM/DD/YYYY HH:MM:SS>]** - Time of Last Update

Selects AutoSupport messages that were last updated at the specified time.

**[-status <AutoSupport general status>]** - Status of Delivery

Selects AutoSupport messages with the status that you specify. Possible values are:

- initializing - The AutoSupport message request is being processed.
- collection-failed - The AutoSupport collection failed. View the 'Last Error' field of this message for more information.
- collection-in-progress - The AutoSupport collection is in progress.
- queued - The AutoSupport message is queued for delivery.
- transmitting - The AutoSupport message transmission is in progress.
- sent-successful - The AutoSupport message was sent successfully.
- ignore - The AutoSupport message was processed successfully, but the trigger event is not configured for delivery to the current destination type.
- re-queued - The AutoSupport message transmission failed, has been re-queued, and will be retried.
- transmission-failed - The AutoSupport message transmission failed, and the retry limit was exceeded.
- ondemand-ignore - The AutoSupport message was processed successfully, but the AutoSupport On Demand server chose to ignore it.

---

**[-attempt-count <integer>]** - Delivery Attempts

Selects AutoSupport messages that the system has attempted to send the number of times you specify. This parameter is most useful when given a range, such as ">5".

**[-subject <text>]** - AutoSupport Subject

Selects AutoSupport messages of the type you specify.

**[-uri <text>]** - Delivery URI

Selects AutoSupport messages sent to the destination URI you specify.

**[-error <text>]** - Last Error

Selects AutoSupport messages that failed with the "Last Error" description you specify.

**[-generated-on <MM/DD/YYYY HH:MM:SS>]** - Time of Generation

Selects AutoSupport messages that were generated (collected) at a particular time.

## Examples

The example below shows the first three results output by the history command. Note that "q" was pressed at the prompt.

```
cluster1::>system node autosupport history show -node node1
Node      Seq  Destination Status          Attempt  Last
-----  ---  -----
node1     56      smtp      ignore          1        11/18/2010 01:10:01
          56      http      re-queued       2        11/18/2010 02:50:07
          56      noteto    transmitting    1        11/18/2010 01:10:01
          55      smtp      ignore          1        11/18/2010 00:53:59
          55      http      sent-successful 3        11/18/2010 01:50:03
          55      noteto    sent-successful 1        11/18/2010 00:53:59
          54      smtp      ignore          1        11/17/2010 12:18:58
          54      http      sent-successful 4        11/17/2010 16:07:22
          54      noteto    sent-successful 1        11/17/2010 12:18:58
Press <space> to page down, <return> for next line, or 'q' to quit... q
9 entries were displayed.
```

---

## system node autosupport manifest show

Display AutoSupport content manifest

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

### Description

The `system node autosupport manifest show` command reports the content of AutoSupport messages. The name and size of each file collected for the message is reported, along with any errors.

### Parameters

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

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

| [-content ]

Displays detailed information about the content of the files contained in the report.

| [-instance ] }

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

[-node {<nodename>|local}] - Node

Selects AutoSupport messages sent from the node you specify.

[-seq-num <Sequence Number>] - AutoSupport Sequence Number

Selects AutoSupport message content with the sequence number you specify. Sequence numbers are unique to a node. Use this parameter with the `-node` parameter to display information about an individual message.

[-prio-num <integer>] - Priority Order of Collection

Selects AutoSupport message content with the collection priority you specify. Content is collected in order, by priority number.

[-sysys <AutoSupport collection subsystems>] - Subsystem

---

Selects AutoSupport message content collected by the AutoSupport subsystem you specify.

**[-cmd-tgt <Execution domain of AutoSupport content>]** - Execution Domain for Command

Selects AutoSupport message content produced in the execution domain you specify.

**[-body-file <text>]** - The AutoSupport Content Filename for this Data

Selects AutoSupport message content stored in the body file with the file name you specify.

**[-cmd <text>]** - Actual Data Being Collected

Selects AutoSupport message content produced by the D-Blade command, BSD command, file, or XML table you specify.

**[-query <text>]** - Table Query for XML Collection

Selects AutoSupport message content produced by the table query you specify.

**[-size-collected {<integer>[KB|MB|GB|TB|PB]}]** - Number of Bytes Collected

Selects AutoSupport message content collected in files with the file size you specify.

**[-time-collected <integer>]** - Collection Time for this Data Item (ms)

Selects AutoSupport message content collected in the amount of time you specify, in milliseconds.

**[-status <AutoSupport manifest collection status>]** - Status of this Data Item

Selects AutoSupport message content with the collection status you specify. Possible values are:

- `requested` - The AutoSupport request has been added to the queue and is waiting processing by the collector.
- `working` - The AutoSupport collector is actively gathering the needed data.
- `file-not-found` - AutoSupport data collection failed because a necessary file is missing.
- `no-such-table` - The AutoSupport collector was unable to find the requested SMF table.
- `collection-truncated-size-limit` - AutoSupport data was truncated due to size limits, but partial data is available.

- 
- `collection-truncated-file-size-limit` - AutoSupport data for a particular data item or file was truncated due to file size limits, but partial data is available.
  - `collection-skipped-size-limit` - AutoSupport data was skipped due to size limits, and no data is available.
  - `collection-truncated-time-limit` - AutoSupport data was truncated due to time limits, but partial data is available.
  - `collection-skipped-time-limit` - AutoSupport data was skipped due to time limits, and no data is available.
  - `delivery-skipped-size-limit` - AutoSupport data was skipped at delivery time due to size limits.
  - `general-error` - AutoSupport data collection failed. Additional information (if any) is in the Error String field.
  - `completed` - AutoSupport data collection is complete, and the AutoSupport message is ready for delivery.
  - `content-not-collected-mode` - AutoSupport content was not collected due to an incompatible operational mode.
  - `content-not-collected-precheck` - AutoSupport content was not collected due to pre-check function violation.
  - `content-not-collected-privacy` - AutoSupport content was not collected because the operation is disabled in privacy mode.
  - `content-empty` - AutoSupport content was collected successfully, but the output was empty.
  - `collection-aborted` - AutoSupport data collection was aborted.

**[-error <text>]** - Textual Description of Error

Selects AutoSupport message content with the error text you specify. If data collection has failed, the error text contains a description of the failure. If data collection completes successfully, this field is empty.

**[-content-type <Type of AutoSupport content>]** - AutoSupport Content Type for this Data

Selects AutoSupport message content of the type you specify. Types supported are:

- `basic` - Configuration data about this subsystem
- `troubleshooting` - Detailed diagnostic data about this subsystem



---

## Examples

The example below displays the content of AutoSupport message number 372 on the node "node1".

```
cluster1::> system node autosupport manifest show -node node1 -seq-num 372
```

Node	Sequence	AutoSupport Body Filename	Collected Size	Status	Error
node1	372				
		SYSCONFIG-A.txt	1.73KB	completed	
		OPTIONS.txt	29.44KB	completed	
		software_image.xml	7.56KB	completed	
		CLUSTER-INFO.xml	3.64KB	completed	
		autosupport.xml	12.29KB	completed	
		autosupport_budget.xml	7.01KB	completed	
		autosupport_history.xml	46.52KB	completed	
		X-HEADER-DATA.TXT	717.00B	completed	
		SYSTEM-SERIAL-NUMBER.TXT	35.00B	completed	
		SOFTWARE-LICENSES.xml	-	content-not-collected-mode	
		cluster_licenses.xml	3.29KB	completed	
		cm_hourly_stats.gz	151.4KB	completed	
		boottimes.xml	56.86KB	completed	
		rdb_txn_latency_stats_hrly.xml	39.31KB	completed	
		rdb_voting_latency_stats_hrly.xml	3.43KB	completed	

15 entries were displayed.

The example below shows how you can use parameters to limit output to specific fields of a specific AutoSupport message. This is helpful when troubleshooting.

```
cluster1::> system node autosupport manifest show -node node5 -seq-num 842 -
fields body-file,status,size-collected,time-collected,cmd,cmd-tgt,subsys
node seq-num prio-num subsys cmd-tgt body-file cmd
size-collected time-collected status
```

node5	842	0	mandatory	dblade	SYSCONFIG-A.txt	"sysconfig -a"
16.44KB		256	completed			
node5	842	1	mandatory	dblade	OPTIONS.txt	options
29.67KB		3542	completed			
node5	842	2	mandatory	smf_table	software_image.xml	software_image
8.68KB		33	completed			
node5	842	3	mandatory	smf_table	CLUSTER-INFO.xml	
asup_cluster_info		4.75KB	7	completed		
node5	842	4	mandatory	smf_table	autosupport.xml	autosupport
12.32KB		10	completed			
node5	842	5	mandatory	smf_table	autosupport_budget.xml	
autosupport_budget		7.03KB	29	completed		
node5	842	6	mandatory	smf_table	autosupport_history.xml	
autosupport_history		62.77KB	329	completed		
node5	842	7	mandatory	custom_fx	X-HEADER-DATA.TXT	"Custom
function"		720.00B	3	completed		
node5	842	8	mandatory	custom_fx	SYSTEM-SERIAL-NUMBER.TXT	"Custom
function"		31.00B	2	completed		
node5	842	9	mandatory	zapi_xml	SOFTWARE-LICENSES.xml	"ZAPI
function"		-	-	content-not-collected-mode		
node5	842	10	mandatory	smf_table	cluster_licenses.xml	
cluster_licenses		5.62KB	9	completed		
node5	842	11	log_files	custom_fx	log_files.xml	"Custom function"
13.07KB		4	completed			
node5	842	12	log_files	custom_fx	EMS-LOG-FILE.gz	"Custom function"
25.33KB		24	completed			
node5	842	13	log_files	dblade_file	EMS-LOG-FILE-PARTNER.gz	/etc/
log/ems -		-	-	content-not-collected-precheck		
node5	842	14	log_files	dblade_file	MESSAGES.gz	/etc/log/messages
35.40KB		42	completed			
node5	842	15	log_files	dblade_file	MESSAGES-PARTNER.gz	/etc/log/
messages -		-	-	content-not-collected-precheck		

---

15 entries were displayed.

---

## system node autosupport trigger modify

Modify AutoSupport trigger configuration

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

### Description

Use the `system node autosupport trigger modify` command to enable and disable AutoSupport messages for individual triggers, and to specify additional subsystem reports to include if an individual trigger sends an AutoSupport message.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node whose AutoSupport trigger configuration is modified.

**-autosupport-message** <Autosupport Message> - EMS Message

Use this parameter to specify the AutoSupport trigger to modify. AutoSupport triggers are EMS messages whose names begin with "callhome.". However, for the purposes of this command, "callhome." is implied, does not need to be entered, and will not be displayed in command output.

**[-to {enabled|disabled}]** - Deliver to AutoSupport -to Addresses

Use this parameter with the value "enabled" to enable sending AutoSupport messages to the configured "to" address.

**[-noteto {enabled|disabled}]** - Deliver to AutoSupport -noteto Addresses

Use this parameter with the value "enabled" to enable sending short notes to the configured "noteto" address.

**[-basic-additional <AutoSupport collection subsystems>, ...]** - Additional Subsystems Reporting Basic Info

Use this parameter to include basic configuration content from the additional subsystems you specify. Content is collected from these subsystems in addition to the default list of subsystems.

**[-troubleshooting-additional <AutoSupport collection subsystems>, ...]** - Additional Subsystems Reporting Troubleshooting Info

---

Use this parameter to include detailed diagnostic content from the additional subsystems you specify. Content is collected from these subsystems in addition to the default list of subsystems.

## Examples

The following example enables messages from the `battery.low` trigger on the node `node1`.

```
cluster1::>> system node autosupport trigger modify -node node1 -autosupport-  
message battery.low -to enabled
```

## See Also

`system node autosupport manifest show`

---

## system node autosupport trigger show

Display AutoSupport trigger configuration

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

### Description

The `system node autosupport trigger show` command displays what system events trigger AutoSupport messages. When a trigger event occurs, the node can send an AutoSupport message to a predefined destination, and a short note to another destination. The full AutoSupport message contains detail for troubleshooting. The short message is meant for short pager or SMS text messages.

Use `system node autosupport destinations show` to view available destinations.

### Parameters

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

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

| **[-basic]** ]

Displays the basic subsystem information that is included when the AutoSupport message is triggered.

| **[-troubleshooting]** ]

Displays which subsystem information is included as troubleshooting information when the AutoSupport message is triggered.

| **[-instance]** }

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

**[-node** {<nodename>|local}] - Node

Selects AutoSupport triggers on the specified node.

**[-autosupport-message** <Autosupport Message>] - EMS Message

---

Selects AutoSupport triggers with the name that you specify. AutoSupport triggers are EMS messages whose names begin with "callhome.". However, for the purposes of this command, "callhome." is implied, does not need to be entered, and will not be displayed in command output.

**[-to {enabled|disabled}]** - Deliver to AutoSupport -to Addresses

Use this parameter with the value "enabled" to select AutoSupport messages that send full messages to the "to" address when triggered. Use this parameter with the value "disabled" to select AutoSupport messages that do not send full messages.

**[-noteto {enabled|disabled}]** - Deliver to AutoSupport -noteto Addresses

Use this parameter with the value "enabled" to select AutoSupport messages that send short notes to the "noteto" address when triggered. Use this parameter with the value "disabled" to select AutoSupport messages that do not send short notes.

**[-basic-default <AutoSupport collection subsystems>, ...]** - Default Subsystems Reporting Basic Info

Selects AutoSupport triggers that include in their messages, by default, basic configuration content from the subsystems you specify.

**[-troubleshooting-default <AutoSupport collection subsystems>, ...]** - Default Subsystems Reporting Troubleshooting Info

Selects AutoSupport triggers that include in their messages, by default, detailed diagnostic content from the subsystems you specify.

**[-additional-content <Type of AutoSupport content>, ...]** - Additional Content Flag

Selects AutoSupport triggers that have been configured to include additional basic or troubleshooting content.

**[-basic-additional <AutoSupport collection subsystems>, ...]** - Additional Subsystems Reporting Basic Info

Selects AutoSupport triggers that have been configured to include additional basic configuration content from the subsystems you specify.

**[-troubleshooting-additional <AutoSupport collection subsystems>, ...]** - Additional Subsystems Reporting Troubleshooting Info

Selects AutoSupport triggers that have been configured to include additional detailed diagnostic content from the subsystems you specify.

## Examples

The example below displays the first page of output from the command. Note that "q" was pressed at the prompt to quit.

---

```
cluster1::>system node autosupport trigger show
```

Node	AutoSupport Message	To	Note To	Additional Content
node1	aggr.offline	enabled	enabled	-
node1	aggr.restricted	disabled	enabled	-
node1	aggr.wafliron	disabled	enabled	-
node1	bad.ram	disabled	disabled	-
node1	battery.failure	enabled	enabled	-
node1	battery.low	disabled	disabled	-
node1	battery.notice	enabled	enabled	-
node1	battery.overchg	enabled	enabled	-
node1	battery.overtemp	enabled	enabled	-
node1	battery.warning	enabled	enabled	-
node1	bmc.bus	disabled	disabled	-
node1	bmc.hb.stop	disabled	disabled	-
node1	bmc.post	disabled	disabled	-
node1	bootfs.chkdisk	enabled	enabled	-
node1	c.fan	enabled	enabled	-
node1	c.fan.fru.degraded	disabled	disabled	-
node1	c.fan.fru.fault	disabled	enabled	-
node1	c.fan.fru.rm	disabled	enabled	-
node1	c.fan.fru.shut	enabled	enabled	-
node1	ch.ps.degraded	disabled	disabled	-

```
Press <space> to page down, <return> for next line, or 'q' to quit... q  
20 entries were displayed.
```

## See Also

`system node autosupport destinations show`   `system node autosupport manifest show`

---

## system node coredump delete-all

Delete all coredumps owned by a node

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

### Description

The `system node coredump delete-all` command deletes either all unsaved core dumps or all saved core files on a node. You can specify whether saved core files or unsaved core dumps are deleted by using the optional `-saved` parameter. If the command is issued while a core dump is being saved, the command prompts you before stopping the save operation and deleting the core dump.

### Parameters

**-node** <nodename> - Node That Owns the Coredump

This specifies the node from which core files or core dumps are to be deleted.

**[-type** {unsaved-kernel|saved-kernel|kernel|application|all}] - Type of Core to delete

This parameter specifies the type of core file to be deleted. If the type is unsaved, all unsaved core dumps will be deleted. If the type is saved, all saved core files will be deleted. If the type is kernel, all kernel core files and kernel core dumps will be deleted. If the type is application, all application core files will be deleted. If the type is all, all core files will be deleted. The default setting is to delete only unsaved kernel core dumps and core files.

### Examples

The following example deletes all unsaved kernel core dumps on a node named node0:

```
cluster1::> system node coredump delete-all -node node0
```

## system node coredump delete

Delete a coredump

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



---

## Description

The `system node coredump delete` command deletes a specified core dump. If the command is issued while the specified core dump is being saved, the command prompts you before stopping the save operation and deleting the core dump.

## Parameters

**-node** {<nodename>|local} - Node That Owns the Coredump

This specifies the node from which core files are to be deleted.

**-type** {kernel|application} - Coredump Type

This specifies the type of core file to be deleted. If the type is kernel, the specified kernel core file will be deleted. If the type is application, the specified application core file will be deleted.

**-corename** <text> - Coredump Name

This specifies the core file that is to be deleted.

## Examples

The following example deletes a core dump named `core.101268397.2010-05-30.19_37_31.nz` from a node named `node0`:

```
cluster1::> system node coredump delete -node node0 -corename
core.101268397.2010-05-30.19_37_31.nz
```

## system node coredump save-all

Save all unsaved kernel coredumps owned by a node

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

## Description

The `system node coredump save-all` saves all unsaved core dumps on a specified node. If the node has already attempted to save the core dump by the value set by the `-save-attempts` parameter, the command prompts you before continuing. The `save-attempts` parameter is set by invoking the command `system node coredump config modify`.

## Parameters

---

**-node** <nodename> - Node That Owns the Coredump

This specifies the node on which unsaved core dumps are to be saved.

## Examples

The following example saves all unsaved core dumps on a node named node0:

```
cluster1::> system node coredump save-all -node node0
```

## See Also

system node coredump save

---

## system node coredump save

Save an unsaved kernel coredump

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

### Description

The `system node coredump save` command saves a specified core dump. If the node has already attempted to save the core dump by the value specified by the `-save-attempts` parameter, the command prompts you before continuing. The `-save-attempts` parameter is set by invoking the command `system node coredump config modify`. A saved core dump can be uploaded to a remote site for support analysis; see the `system node coredump upload` command man page for more information.

### Parameters

**-node** {<nodename>|local} - Node That Owns the Coredump

This specifies the node on which the core dump is located.

**-corename** <text> - Coredump Name

This specifies the core dump that is to be saved.

### Examples

The following example saves a core dump named `core.101268397.2010-05-30.19_37_31.nz` on a node named `node0`:

```
cluster1::> system node coredump save -node node0 -corename  
core.101268397.2010-05-30.19_37_31.nz
```

### See Also

`system node coredump config modify`   `system node coredump upload`  
`system node coredump save-all`

---

## system node coredump show

Display a list of coredumps

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

### Description

The `system node coredump show` command displays information about core dumps, such as the core dump name, time of panic that triggered the core dump and whether the core file is saved. You can specify optional parameters to display information that matches only those parameters. For example, to display the list of kernel core files, run the command with `-type kernel`.

### Parameters

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

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

| **[-system ]**

Displays the following information:

- Node name
- Core dump name
- Core dump ID
- Node that panicked and generated the core
- System ID of the node that panicked and generated the core
- Version of the core

| **[-instance ] }**

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

**[-node {<nodename>|local}]** - Node That Owns the Coredump

---

Selects information about the core files on the specified node. If you specify both this parameter and the `-corename` parameter, the command displays detailed information about the specified core.

**[-type {kernel|application}]** - Coredump Type

Selects the type of core files to be displayed. If the type is kernel, the command displays kernel core files. If the type is application, the command displays application core files.

**[-corename <text>]** - Coredump Name

Selects information about the core files that match the specified name. If you specify both this parameter and the `-node` parameter, the display includes detailed information about the specified core.

**[-panic-node <text>]** - Node That Generated Core

Selects information about the core files that were generated when the specified node panicked.

**[-panic-systemid <integer>]** - System ID of Node That Generated Core

Selects information only about the core files that were generated when the specified node panicked.

**[-version <text>]** - Data ONTAP Version of Core

Selects information only about core files that match the specified version.

**[-panic-time <MM/DD/YYYY HH:MM:SS>]** - Time of Panic That Generated Core

Selects information about the core files that were generated by a panic at the specified time. Specify time in the format of MM/DD/YYYY HH:MM:SS [+ HH:MM]. You can use [+ HH:MM] to specify the time range relative to UTC

**[-panic-string <text>]** - Panic String

Selects information about core files that match the specified panic string.

**[-is-saved {true|false}]** - Saved Core

If you specify this parameter, the command displays information only about the core dumps that are or are not saved yet to a core file.

**[-is-partial {true|false}]** - Partial Core

Selects information about core dumps that are or are not partially saved.

**[-save-attempts <integer>]** - Number of Attempts to Save Core

Selects information about core dumps that have the specified number of successful or failed save attempts.

---

**[-space-needed {<integer>[KB|MB|GB|TB|PB]]** - Space Needed To Save Core

Selects information about core dumps that need the specified amount of disk space to save into a core file.

**Examples**

The examples below display information about the core files:

```
cluster1::> system node coredump show
Node   Core Name                               Saved   Panic Time
-----
node0
  core.101182345.2010-02-01.14_19_08.nz      false   2/1/2010 09:19:08
    Partial Core: false
    Number of Attempts to Save Core: 2
    Space Needed To Save Core: 4.45GB
node1
  core.101268397.2010-05-30.19_37_31.nz      true    5/30/2010 15:37:31
node2
  core.101270930.2010-09-06.18_40_03.nz      true    9/6/2010 14:40:03
node3
  core.101271326.2010-09-06.19_06_18.nz      true    9/6/2010 15:06:18
  core.101271326.2010-09-06.19_09_49.nz      true    9/6/2010 15:09:49
4 entries were displayed.

cluster1::> system node coredump show -panic-time 9/6/2010 15:00:00+3:00
Node   Core Name                               Saved   Panic Time
-----
node3
  core.101271326.2010-09-06.19_06_18.nz      true    9/6/2010 15:06:18
  core.101271326.2010-09-06.19_09_49.nz      true    9/6/2010 15:09:49
2 entries were displayed.
```

**See Also**

system node coredump status

---

## system node coredump status

Display kernel coredump status

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

### Description

The `system node coredump status` command displays status information about core dumps. The command output depends on the parameters specified with the command. If a core dump is in the process of being saved into a core file, the command also displays its name, the total number of blocks that are to be saved, and the current number of blocks that are already saved.

You can specify additional parameters to display only information that matches those parameters. For example, to display coredump status information about the local node, run the command with the parameter `-node local`.

Some parameters are available only at the advanced privilege level and higher.

### Parameters

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

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

| **[-disks ]** (privilege: advanced)

If you specify this parameter, the command displays the following information:

- Node name
- Total number of disks
- Number of spare disks
- Number of disks used
- Number of disks with partial cores

This parameter is available only at the advanced privilege level and higher.

| **[-spraycore ]** (privilege: advanced)

If you specify this parameter, the command displays the following information:

- 
- Node name
  - Whether spray cores are supported
  - Number of spray-core disks
  - Number of spray-core blocks
  - Number of disks needed for spray core
  - Number of blocks needed for spray core

This parameter is available only at the advanced privilege level and higher.

| [-instance ] }

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

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays the following information:

- Node name
- State of the core-dump process
- Space available on the internal file system
- Name of the core being saved, if applicable
- Total number of blocks in the core being saved, if applicable
- Number of blocks currently saved, if applicable
- Type of core dump
- Number of unsaved complete cores on the node
- Number of unsaved partial cores on the node

If you specify this parameter at the advanced privilege level or higher, the command displays the following additional information:

- Whether spray cores are supported on the node
- Whether any spare disks are available on the node
- Number of disks that have cores
- Number of unsaved cores
- Number of disks that have partial cores



- 
- Number of partial cores
  - Number of unused spray-core disks
  - Number of spray-core blocks
  - Number of disks available for core dumps
  - Number of blocks needed for spray core
  - Number of disks needed for spray core

**[-state <text>]** - State

If you specify this parameter, the command displays information only about the nodes that are in the specified core dump state. Possible values include: nocore, idle, init, saving, and waitdump.

**[-space-available {<integer>[KB|MB|GB|TB|PB]}]** - Space Available On Internal Filesystem

If you specify this parameter, the command displays information only about the nodes that have the specified amount of available space, in bytes, on their internal file systems.

**[-corename <text>]** - Name of Core Being Saved

If you specify this parameter, the command displays information only about the node that is currently saving the specified core file name.

**[-total-blocks <integer>]** - Total Number of Blocks in Core Being Saved

If you specify this parameter, the command displays information only about the nodes that have the specified number of blocks in the core dump being saved.

**[-blocks-saved <integer>]** - Number of Blocks saved

If you specify this parameter, the command displays information only about the nodes that have the specified number of blocks saved.

**[-type <text>]** - Type of Core Dump

If you specify this parameter, the command displays information only about the nodes that have the specified core dump type. Possible values include zipped, sprayed, and spare.

**[-spraycore-supported {true|false}]** - Spray Core Supported on Node (privilege: advanced)

---

If you specify this parameter, the command displays information only about the nodes that do or do not support the spray method of dumping core. This parameter is available only at the advanced privilege level and higher.

**[-spares-available {true|false}]** - Spare Disk(s) Available on Node (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that do or do not have spare disks available. This parameter is available only at the advanced privilege level and higher.

**[-disks-used <integer>]** - Number of Disks with Cores (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of disks that contain core dumps. This parameter is available only at the advanced privilege level and higher.

**[-unsaved-cores <integer>]** - Number of Unsaved Complete Cores

If you specify this parameter, the command displays information only about the nodes that have the specified number of complete core dumps that are not yet saved into a core file.

**[-partial-disks <integer>]** - Number of Disks with Partial Cores (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of disks with partial core dumps. This parameter is available only at the advanced privilege level and higher.

**[-partial-cores <integer>]** - Number of Unsaved Partial Cores

If you specify this parameter, the command displays information only about the nodes that have the specified number of partial core dumps that are not yet saved into a core file.

**[-spraycore-disks <integer>]** - Number of Unused Spray Core Disks (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of unused spray-core disks. This parameter is available only at the advanced privilege level and higher.

**[-spraycore-blocks <integer>]** - Number of Spray Core Blocks (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of spray-core blocks. This parameter is available only at the advanced privilege level and higher.

**[-numdisks <integer>]** - Total Number of Disks Available for Core Dump (privilege: advanced)

---

If you specify this parameter, the command displays information only about the nodes that have the specified total number of disks available for core dump. This parameter is available only at the advanced privilege level and higher.

**[-blocks-needed <integer>]** - Number of Blocks Needed for Spray Core (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of blocks needed for the spray method of dumping core. This parameter is available only at the advanced privilege level and higher.

**[-disks-needed <integer>]** - Number of Disks Needed for Spray Core (privilege: advanced)

If you specify this parameter, the command displays information only about the nodes that have the specified number of disks needed for the spray method of dumping core. This parameter is available only at the advanced privilege level and higher.

**[-space-needed {<integer>[KB|MB|GB|TB|PB]}]** - Space Needed to Save All Unsaved Cores

If you specify this parameter, the command displays information only about the nodes that require the specified amount of disk space to save all unsaved core dumps.

**[-min-free {<integer>[KB|MB|GB|TB|PB]}]** - Minimum Free Bytes on Root Filesystem

If you specify this parameter, the command displays information only about the nodes that need to have the specified number of bytes available on the root filesystem after a core dump is saved.

## Examples

The following example displays core dump information about the node named node0:

```
cluster1::> system node coredump status -node node0 -instance
Node: node0
State: idle
Space Available On Internal Filesystem: 132.1GB
Name of Core Being Saved: -
Total Number of Blocks in Core Being Saved: -
Number of Blocks saved: -
Type of core dump: spray
Number of Unsaved Complete Cores: 0
Number of Unsaved Partial Cores: 1
Space Needed To Save All Unsaved Cores: 4.81GB
Minimum Free Bytes On Internal Filesystem: 250MB
```

## See Also

system node coredump show

---

## system node coredump upload

Upload a coredump to a remote site

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node coredump upload` command uploads a saved core file to a specified URL. You should use this command only at the direction of technical support.

### Parameters

**-node** {<nodename>|local} - Node That Owns the Coredump

This specifies the node on which the core file is located.

**-type** {kernel|application} - Coredump Type

This specifies the type of core files to be uploaded. If the type is kernel, kernel core files will be uploaded. If the type is application, application core file will be uploaded.

**-corename** <text> - Coredump Name

This specifies the name of the core file that is to be uploaded.

**[-location <text>]** - URL for Coredump Upload Directory

This specifies the URL to which the core file is to be uploaded. If this parameter is not specified, the command uploads the core file to the location specified by the `-upload-location` parameter of the `system node coredump config modify` command. The following protocols are supported: ftp, tftp, and http. (By default, the location is set to `ftp://ftp.netapp.com/to-ntap/`)

**[-casenum <integer>]** - Case Number

This specifies the support case number that will be prefixed to the core file name at the destination. The case number is critical information for quick and automated processing of the received core file.

### Examples

The following example uploads a core file named `core.07142005145732.2010-10-05.19_03_41.nz` on a node named `node0` to the default location. The support case number is `2001234567`.

---

```
cluster1::> system node coredump upload -node node0 -corename  
core.07142005145732.2010-10-05.19_03_41.nz -casenum 2001234567
```

## See Also

[system node coredump config modify](#)

---

## system node coredump config modify

Modify coredump configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node coredump config modify` command modifies the cluster's core dump configuration.

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node whose coredump configuration you want to modify.

**[-sparsecore-enabled** {true|false}] - Enable Sparse Cores

If you set this parameter to true, the command enables sparse cores. A sparse core omits all memory buffers that contain only user data.

**[-min-free** {<integer>[KB|MB|GB|TB|PB]}) - Minimum Free Bytes On Root Filesystem

If you specify this parameter, the command displays the number of bytes that need to be made available in the root file system after saving the core dump. If the minimum number of bytes cannot be guaranteed, core dumps are not generated. The default setting is 250 MB.

**[-coredump-attempts** <integer>] - Maximum Number Of Attempts to Dump Core

If you specify this parameter, the command displays the maximum number of times the system will attempt to generate a core dump when encountering repeated disk failures. The default setting is 2.

**[-save-attempts** <integer>] - Maximum Number Attempts to Save Core

If you specify this parameter, the command displays the maximum number of times the system will attempt to save a core dump. The default setting is 2.

**[-save-onstartup** {true|false}] - Enable Auto Save of Coredumps on Startup

If you set this parameter to true, the system will automatically start saving the core dump after reboot.

**[-upload-location** <text>] - URL for Coredump Upload Directory

---

If you specify this parameter, the system uploads the core dumps to the specified URL. The following protocols are supported: ftp, tftp, and http. (The default setting is ftp://ftp.netapp.com/to-ntap/.)

## Examples

The following example sets the maximum number of core dump attempts to 5 and the maximum number of save attempts to 5:

```
cluster1::> system node coredump config modify -coredump-attempts 5 -save-attempts 5
```

## system node coredump config show

Display coredump configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system node coredump config show` command displays basic information about a cluster's core dump configuration, such as whether sparse cores are enabled, minimum number of free bytes on the root volume file system that need to be available after saving the core files, maximum number of times the process attempts to generate a core dump when encountering repeated disk failures, maximum number of times the process attempts to save a core dump, the URL to which core dumps are uploaded, and whether core dumps are automatically saved when a node restarts.

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**node** {<nodename>|local}] - Node

Selects the coredump configuration information of the specified node.

[-**sparsecore-enabled** {true|false}] - Enable Sparse Cores

Selects the coredump information that matches the specified spare core setting. A sparse core omits all memory buffers that contain only user data.

**[-min-free {<integer>[KB|MB|GB|TB|PB]}]** - Minimum Free Bytes On Root Filesystem

Selects the core dump information that matches the specified number of bytes that need to be made available in the root file system after saving the core dump.

**[-coredump-attempts <integer>]** - Maximum Number Of Attempts to Dump Core

Selects the core dump information that matches the specified maximum number of times the system will attempt to generate a core dump when encountering repeated disk failures.

**[-save-attempts <integer>]** - Maximum Number Attempts to Save Core

Selects the coredump information that matches the maximum number of times the system will attempt to save a core dump.

**[-save-onstartup {true|false}]** - Enable Auto Save of Coredumps on Startup

Selects the coredump information that matches the specified configuration of whether the system will automatically start saving the core dump after reboot.

**[-upload-location <text>]** - URL for Coredump Upload Directory

Selects the core dump information that matches the specified URL where core dumps are uploaded.

## Examples

The example below displays information about the cluster's core dump configuration:

```
cluster1::> system node coredump config show
      Sparse      Min      Max      Max
      Core      Free      Dump      On
Node  Enabled    Bytes  Attempts  Attempts  Save  Startup  Coredump Location
-----
node0  true      250MB      2          2      true  true      ftp://ftp.example.com/to-
example/
node1  true      250MB      2          2      true  true      ftp://ftp.example.com/to-
example/
node2  true      250MB      2          2      true  true      ftp://ftp.example.com/to-
example/
node3  true      250MB      2          2      true  true      ftp://ftp.example.com/to-
example/
4 entries were displayed.
```



---

## system node coredump reports delete

Delete an application core report

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node coredump reports delete` command deletes the specified application core report.

### Parameters

**-node** {<nodename>|local} - Node That Owns the Coredump

This specifies the node from which reports are to be deleted.

**-reportname** <text> - Report Name

This specifies the report that is to be deleted.

### Examples

The following example shows how a report named `notifyd.1894.80335005.2011-03-25.09_59_43.ucore.report` is deleted from a node named `node0`:

```
cluster1::> system node coredump reports delete -node node0 -reportname  
notifyd.1894.80335005.2011-03-25.09_59_43.ucore.report
```

## system node coredump reports show

Display a list of application core reports

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node coredump reports show` command displays basic information about application core reports, such as the report name and time of the panic that triggered the application core dump. You can specify optional parameters to display

---

information that matches only those parameters. For example, to display the list of reports in the local node, run the command with `-node local`.

## Parameters

**{ [-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node That Owns the CoreDump

Selects information about all the reports on the specified node. If you specify both this parameter and the `-reportname` parameter, the command displays detailed information about the specified report.

**[-reportname <text>]** - Report Name

Selects information about the reports that match the specified name. If you specify both this parameter and the `-node` parameter, the command displays detailed information about the specified report.

**[-panic-node <text>]** - Node That Generated Core

Selects information about the reports that were generated by the specified node.

**[-panic-systemid <integer>]** - System ID of Node That Generated Core

Selects information about the reports that were generated by the node with the specified system ID.

**[-version <text>]** - Data ONTAP Version of Core

Selects information about the reports that match the specified version.

**[-panic-time <MM/DD/YYYY HH:MM:SS>]** - Time of Panic That Generated Core

Selects information about the reports that were generated by a panic at the specified time. Specify time in the format of `MM/DD/YYYY HH:MM:SS` [`+/- HH:MM`]. You can use [`+/- HH:MM`] to specify the time range within which all core files triggered by a panic are displayed. [`+/- HH:MM`] is relative to UTC.

**[-panic-string <text>]** - Panic String

Selects information about the reports that match the specified panic string.

---

## Examples

The following example displays information about the reports:

```
cluster1::> system node coredump reports show
Node      Report Name                                     Panic Time
-----
node0     notifyd.1894.80335005.2011-03-25.09_59_43.ucore.report  3/25/2011
09:59:43
```

---

## system node coredump reports upload

Upload an application core report to a remote site

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node coredump reports upload` command uploads an application report to a specified URL. You should use this command only at the direction of technical support.

### Parameters

**-node** {<nodename>|local} - Node That Owns the Coredump

This specifies the node on which the report is located.

**-reportname** <text> - Report Name

This specifies the name of the report that is to be uploaded.

**[-location** <text>] - URL for Coredump Upload Directory

This specifies the URL to which the report is to be uploaded. The following protocols are supported: ftp, tftp, and http. (By default, the location is set to ftp://ftp.netapp.com/to-ntap/)

**[-casenum** <integer>] - Case Number

This specifies the support case number that is be prefixed to the core file name at the destination. The case number is critical information for quick and automated processing of the received core file.

### Examples

The following example shows how a report named `notifyd.1894.80335005.2011-03-25.09_59_43.ucore.bz2` is uploaded on a node named `node0` to the default location. The support case number is `2001234567`.

```
cluster1::> system node coredump reports upload -node node0 -corename  
notifyd.1894.80335005.2011-03-25.09_59_43.ucore.bz2 -casenum 2001234567
```

---

## system node coredump segment delete-all

Delete all core segments on a node

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command deletes all the core segments on a node.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which to delete the core segments.

### Examples

This deletes all the core segments for node1.

```
cluster1::>system node coredump segment delete-all -node node1
```

## system node coredump segment delete

Delete a core segment

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command deletes a core segment.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which to delete the core segments.

**-segment** <text> - Core Segment

---

This specifies the core segment to delete. The pathname is relative to the coredump directory. If a directory is specified, all core segment files within it are deleted. If the directory is empty, it is deleted.

**[-owner-node <text>]** - Node That Owns the Core Segment File

This specifies the node that owns the core segment. Use this parameter only in takeover mode to delete a partner's coredump segment.

## Examples

This deletes all core segments in the directory, core.151708240.2012-01-11.05\_56\_52.

```
cluster1::>system node coredump segment delete -node node1 -segment  
core.151708240.2012-01-11.05_56_52
```

## system node coredump segment show

Display a list of core segments

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

This command displays the following information about core segments:

- name of the core segment directory
- time of the panic that generated the core segment
- total number of core segment files
- core segment file name

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the **-fields <fieldname>, ...** parameter, the command output also includes the specified field or fields. You can use **-fields ?** to display the fields to specify.

| **[-instance ]** }

Displays the following details:

- Core segment file name

- 
- Node that owns the core segment file
  - System ID of the node that generated the core
  - MD5 checksum of the compressed data of the core segment file
  - Name of the core segment
  - Total number of core segments for the core file
  - Timestamp of the panic that triggered the core segment

**[-node {<nodename>|local}]** - Node

Selects information about the core segments on the specified node.

**[-segment <text>]** - Core Segment

Selects information about the specified core segment. If segment is a directory, the command displays the information for the first core segment file. If segment is a file, the command displays the file information.

**[-owner-node <text>]** - Node That Owns the Core Segment File

Selects information about the core segments owned by the specified node. This parameter should only be used in takeover mode to display information about the partner's core segments.

**[-panic-system-id <integer>]** - System ID of Node That Generated Core

Selects information about the core segments that were generated when the node with the specified system ID panicked.

**[-md5-data-chksum <text>]** - Md5 Checksum of the Compressed Data of the Core Segment

Selects information about the core segments whose data segment's MD5 checksum matches the specified checksum.

**[-segment-name <text>]** - Name of the Core Segment

Selects information about the core segments with the specified name.

**[-total-segment-count <integer>]** - Number of Segments Generated

Selects information about the core segments with the specified name.

**[-panic-time <MM/DD/YYYY HH:MM:SS>]** - Time of Panic That Generated Core

Selects information about the core segments that were generated by a panic at the specified time.

---

## Examples

The example below displays the core segments on node1.

```
cluster1::> system node coredump segment show -node node1
Node: node1
    Segment Directory: core.118049106.2012-01-05.17_11_11
    Panic Time: 1/5/2012 12:11:11
    Number of Segments: 2
    Segment File Name:
        core.118049106.2012-01-05.17_11_11.nvram.nz
        core.118049106.2012-01-05.17_11_11.ontap.nz
2 entries were displayed.
```

The example below displays detailed information a specific core segment file on node1.

```
cluster1::>system node coredump segment show -node node1 -segment
core.118049106.2012-01-05.17_11_11.ontap.nz -instance
Node: node1
Core Segment:
core.118049106.2012-01-05.17_11_11.ontap.nz
    Node That Owns the Core Segment File: node1
    System ID of Node That Generated Core: 118049106
Md5 Checksum of the Compressed Data of the Core Segment:
1a936d805dcd4fd5f1180fa6464fdee4
    Name of the Core Segment: ontap
    Number of Segments Generated: 2
    Time of Panic That Generated Core: 1/5/2012 12:11:11
```



---

## system node coredump segment start

Start a core segmenting job

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command schedules a job to segment a core file.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which you want to segment the core file.

**-core-name** <text> - Name of the Full Core to Be Segmented

This specifies the core file to segment.

**[-delete-core {true|false}]** - Deletes Full Core After Successful Segmenting of the Core

This specifies to delete the full core file after the segmenting. The default is false - do not delete.

### Examples

This schedules a job to segment the core file, core.101166076.2012-01-22.18\_38\_09.nz on node1.

```
cluster1::>system node coredump segment start -node node1 -corename  
core.101166076.2012-01-22.18_38_09.nz
```

## system node coredump segment status

Display status of a core segmenting job

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the status of a core segmenting job. The following fields are displayed:

- 
- Job Id
  - Core file name
  - Status
  - Percentage complete

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**node** {<nodename>|local}] - Node

This displays detailed information for all core segmenting jobs.

[-**core-name** <text>] - Name of the Full Core to Be Segmented

If you specify this parameter, the command displays only the status for the core segmenting job that is segmenting the specified core name.

[-**owner-node** <text>] - Node Whose Full Core Will Be Segmented

If you specify this parameter, the command displays only the status for core segmenting jobs whose core file is owned by the specified node. This parameter should only be used in takeover mode to display information about the partner's core segments.

[-**job-id** <integer>] - Core Segmenting Job Id

If you specify this parameter, the command displays only the status for the core segmenting job identified by the job id.

[-**status** <The status fo the core segmentation job>] - Status of the Core Segmenting Job

If you specify this parameter, the command displays information only for the core segmenting jobs that have the specified status.

Statuses :

- Queued - The job is in the queue. It might run immediately or it might run after another job completes.

- 
- Running - The job is running.
  - Stopping - The job has been canceled.

**[-percent-completed <percent>]** - Percentage of the Core Segmentation Completed

If you specify this parameter, the command displays only the status of core segmenting jobs that are (at least) a specific percent complete.

## Examples

This displays the status of the core segmenting jobs on node1.

```
cluster1:::>system node coredump segment status -node node1
```

Node	ID	Core Name	Status	Percent
----	--	-----	-----	-----
node1	1	core.118049106.2012-01-05.17_11_11.nz	Running	15%

---

## system node coredump segment stop

Cancel core segmenting job

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command cancels a core segmenting job.

### Parameters

**-node** {<nodename>|local} - Node

This is the node on which the core segmenting job is running.

**-job-id** <integer> - Core Segmenting Job Id

This is the job identifier of the core segmenting job.

### Examples

This cancels core segmenting job 10 on node1.

```
cluster1:::>system node coredump segment stop -node node1 -job-id 10
```

## system node coredump segment config modify

Modify the core segmenting configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command controls automatic core file segmenting.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node whose core segmenting configuration is updated.

---

**[-auto-delete {true|false}]** - Enable Deletion of Full Core After Automatic Core Segmenting

This specifies whether the core file is deleted after automatic segmentation.

The default setting is false - do not delete the core file.

**[-auto-segment {true|false}]** - Enable Automatic Core Segmenting After Saving of a Full Core

This specifies whether the core file is automatically segmented after it is saved.

In some systems, the default setting is false. For all other platforms, the default setting is true - the system will automatically segment the full core file after the core has been saved.

## Examples

This enables automatic core file segmenting.

```
cluster1::> system node coredump segment modify -node nodel -auto-segment true
```

## system node coredump segment config show

Display the core segmenting configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

This command displays basic information about a node's core segmenting configuration, such as whether automatic segmenting is enabled and whether the full core file is deleted afterward.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the **-fields <fieldname>, ...** parameter, the command output also includes the specified field or fields. You can use **-fields ?** to display the fields to specify.

| **[-instance ]** }

Displays detailed information about all entries.

**[-node {<nodename>|local}]** - Node

---

Selects the nodes for which information is displayed.

**[-auto-delete {true|false}]** - Enable Deletion of Full Core After Automatic Core Segmenting

Selects information about nodes that match the specified configuration for auto-delete (whether the full core file should be automatically segmented after it is saved).

**[-auto-segment {true|false}]** - Enable Automatic Core Segmenting After Saving of a Full Core

Selects information about nodes that match the specified configuration for auto-segment (whether the full core file should be automatically segmented after it is saved).

## Examples

The example below displays the core segmenting configuration for all nodes in the cluster.

```
cluster1::> system node coredump segment config show -node *
Node           AutoSegment  AutoDelete
-----
cluster1       true          true
```

---

## system node environment sensors show

Display the sensor table

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node environment sensors show` command displays the following information:

- Node name
- Sensor name
- Sensor state
- Sensor value
- Sensor units
- Critically Low threshold for the sensor
- Warning Low threshold for sensor
- Warning High threshold for sensor
- Critically High threshold for the sensor
- FRU name (detailed view only)

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

---

Selects information about the sensors on the specified node. If this parameter is specified with the `-name` parameter, the command displays information only about the specified sensor.

**`[-name <text>]`** - Sensor Name

Selects information about the sensors that have the specified name. If this parameter is specified with the `-node` parameter, the command displays information only about the specified sensor.

**`[-fru <text>]`** - FRU

Selects information about the sensors associated with the specified Field Replaceable Unit (FRU).

**`[-type <text>]`** - Sensor Type

Selects information about the sensors that have the specified sensor type. Possible values vary among platforms but may include fan, temperature, thermal and voltage.

**`[-units <text>]`** - Value Units

Selects information about the sensors that have readings displayed in the specified units of measure. Possible values vary among platforms but may include RPM, C and mV.

**`[-state <text>]`** - Sensor State

Selects information about the sensors that have the specified state. Possible values vary among platforms but may include normal, warn\_lo, warn\_hi, crit\_lo, crit\_hi and failed.

**`[-discrete-state <text>]`** - Discrete Sensor State

Selects information about the discrete-valued sensors that are in the specified state. A discrete-valued sensor has a set of possible discrete values rather than a range of possible values. For example, a presence sensor which has the discrete values PRESENT and NOT\_PRESENT is a discrete-valued sensor. Possible values vary among platforms but may include normal and failed.

**`[-value <integer>]`** - Last Sensor Value

Selects information about the sensors that have the specified sensor value.

**`[-discrete-value <text>]`** - Discrete Sensor Value

Selects information about the discrete-valued sensors that have the specified discrete value. Possible values vary among sensors but may include PRESENT, NOT\_PRESENT, ON, OFF, OK and FAULT.

**`[-crit-low <integer>]`** - Critical Low Threshold



Selects information about the sensors that have the specified critically low threshold.

**[-warn-low <integer>]** - Warning Low Threshold

Selects information about the sensors that have the specified warning-low threshold.

**[-warn-hi <integer>]** - Warning Hi Threshold

Selects information about the sensors that have the specified warning-high threshold.

**[-crit-hi <integer>]** - Critical Hi Threshold

Selects information about the sensors that have the specified critically high threshold.

**[-inactive {true|false}]** - Show Inactive Sensors

Selects information about the sensors that are currently inactive.

## Examples

The following example displays information about all sensors on a cluster named cluster1:

```
cluster1::> system node environment sensors show
Node Sensor                               State Value/Units Crit-Low Warn-Low Warn-Hi Crit-Hi
-----
mynode
  Partner IO Pre                          NOT_PRESENT
  Partner Ctrl Pre                        PRESENT
  PSU2 Over Curr                          OK
  PSU2 Over Volt                          OK
  PSU2 Over Temp                          OK
  PSU2 Fault                              OK
  PSU2 DC OK                              OK
  PSU2 Input OK                           OK
  PSU2 ON                                 ON
  PSU2 Fan2 Fault                         OK
Node Sensor                               State Value/Units Crit-Low Warn-Low Warn-Hi Crit-Hi
-----
mynode
  PSU2 Fan2 Speed                         normal 15400 RPM    3000    3500    -    25500
  PSU2 Fan1 Fault                         OK
  PSU2 Fan1 Speed                         normal 15700 RPM    3000    3500    -    25500
  PSU2 Curr                              normal 28000 mA      -      -      -      -
  PSU2 Temp                              normal 29 C          0       5      51     61
  PSU2 Present                           PRESENT
  PSU1 Over Curr                          OK
  PSU1 Over Volt                          OK
  PSU1 Over Temp                          OK
```

---

Node	Sensor	State	Value/Units	Crit-Low	Warn-Low	Warn-Hi	Crit-Hi
-----							
mynode							
	PSU1 Fault		OK				
	PSU1 DC OK		OK				
	PSU1 Input OK		OK				
	PSU1 ON		ON				
	PSU1 Fan2 Fault		OK				
	PSU1 Fan2 Speed	normal	15600 RPM	3000	3500	-	25500
	PSU1 Fan1 Fault		OK				
	PSU1 Fan1 Speed	normal	16200 RPM	3000	3500	-	25500
	PSU1 Curr	normal	27000 mA	-	-	-	-
	PSU1 Temp	normal	28 C	0	5	51	61
-----							
Node	Sensor	State	Value/Units	Crit-Low	Warn-Low	Warn-Hi	Crit-Hi
-----							
mynode							
	PSU1 Present		PRESENT				
	Battery 3.3V	normal	3400 mV	3025	3100	3500	3575
	AUX 3.3V	normal	3328 mV	3024	3104	3504	3568
	STBY 12V	normal	12152 mV	10478	10602	13392	13516
	STBY 5V	normal	4979 mV	4602	4696	5310	5404
	STBY 3.3V	normal	3375 mV	3025	3100	3500	3575
	12V	normal	12152 mV	10478	10726	13268	13516
	5V	normal	5003 mV	4602	4696	5310	5404
	3.3V	normal	3375 mV	3025	3100	3500	3575
[...]							

---

---

## system node firmware download

Download motherboard firmware and system diagnostics

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system node firmware download` command downloads new system firmware to the boot device. A reboot followed by the 'update\_flash' command at the firmware prompt is required for the firmware to take effect.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node or nodes on which the firmware is to be updated.

**-package** <text> - Package URL

This parameter specifies the URL that provides the location of the package to be fetched. Standard URL schemes, including HTTP, FTP, TFTP and FILE, are accepted.

### Examples

The following example downloads firmware to node-01 from a web server:

```
node-01::*> system node firmware download -node node-01 -package
http://example.com/serviceimage.zip
```

## system node hardware tape drive show

Displays information about tape drives

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the following information about tape drives:

- Node to which the tape drive is attached
- Device ID of the tape drive

- Description of the tape drive
- NDMP path of the tape drive

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

Displays detailed information about tape drives on the specified node.

[-device-id <text>] - Device ID

Selects information about the tape drive that has the specified device ID.

[-description <text>] - Description

Selects information about the tape drive or drives that have the specified description.

[-wwn <text>] - World Wide Name

Selects information about the tape drive that has the specified worldwide name.

[-serial-number <text>] - Serial Number

Selects information about the tape drive that has the specified serial number.

[-ndmp-path <text>, ...] - NDMP Path

Selects information about the tape drive or drives that have the specified NDMP path.

## Examples

The following example displays information about all tape drives in the cluster:

```
cluster1::> system node hardware tape drive show
Node   Device Id Drive Description NDMP Path
-----
cluster1
  brocade-247-198:3.126L1      nrst0l nrst0m nrst0h nrst0a
    IBM LTO 4 ULTRIUM          rst0l rst0m rst0h rst0a
    urst0l urst0m urst0h urst0a
  brocade-247-198:3.126L2      nrst1l nrst1m nrst1h nrst1a
    IBM LTO 4 ULTRIUM          rst1l rst1m rst1h rst1a
    urst1l urst1m urst1h urst1a
  brocade-247-198:3.126L3      nrst2l nrst2m nrst2h nrst2a
    IBM LTO 4 ULTRIUM          rst2l rst2m rst2h rst2a
    urst2l urst2m urst2h urst2a
```

---

brocade-247-198:3.126L4	nrst3l nrst3m nrst3h nrst3a
IBM LTO 4 ULTRIUM	rst3l rst3m rst3h rst3a
	urst3l urst3m urst3h urst3a
brocade-247-198:3.126L6	nrst5l nrst5m nrst5h nrst5a
SONY SDX-400C	rst5l rst5m rst5h rst5a
	urst5l urst5m urst5h urst5a

5 entries were displayed.

---

## system node hardware tape library show

Display information about tape libraries

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the following information about tape libraries:

- Node to which the tape library is attached
- Device ID of the tape library
- Description of the tape library
- NDMP path of the tape library

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Displays detailed information about tape libraries on the specified node.

**[-device-id <text>]** - Device ID

Selects information about the tape library that has the specified device ID.

**[-description <text>]** - Description

Selects information about the tape library or libraries that have the specified description.

**[-wwn <text>]** - World Wide Name

Selects information about the tape library that has the specified worldwide name.

**[-serial-number <text>]** - Serial Number

---

Selects information about the tape library that has the specified serial number.

**[-ndmp-path <text>]** - NDMP Path

Selects information about the tape library or libraries that have the specified NDMP path.

**Examples**

The following example displays information about all tape libraries attached to the cluster:

```
cluster1::> system node hardware tape library show
Node      Device Id Drive Description      NDMP Path
-----
cluster1-00
      0b.125L1  HP      MSL G3      mc1
              Series
      0c.125L1  HP      MSL G3      mc0
              Series
2 entries were displayed.
```

---

## system node image get

Fetch a file from a URL

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command fetches a file from the specified URL and stores it in the `/etc/software` directory.

### Parameters

**[-node {<nodename>|local}]** - Node

This parameter specifies the node that will fetch and store the package.

**-package <text>** - Package URL

This parameter specifies the URL that provides the location of the package to be fetched. Standard URL schemes, including HTTP, FTP, TFTP and FILE, are accepted.

**[-replace-package [true]]** - Replace the Local File

Specifies whether an existing package is deleted and replaced with a new package. If you enter this command without using this parameter, its effective value is false and an existing package is not replaced with the new one. If you enter this parameter without a value, it is set to true and an existing package is replaced with the new one.

**[-rename-package <text>]** - Rename the File

Use this parameter to enter a package name that is different than the file name in the URL.

**[-background [true]]** - Run in the background

This parameter will allow the operation to run in the background. The progress of the operation can be checked with the command `system image show-update-progress`. If this command is entered without using this parameter, its effective value is false and the operation will run in the foreground. If this parameter is used without a value, it is set to true.

### Examples

```
system image get http://example.com/image.tgz -rename-package image2.tgz -  
replace-package
```



---

## system node image modify

Modify software image configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node image modify` command sets the default software image on a specified node. The default software image is the image that is run when the node is started. A node holds two software images; when you set one as the default image, the other image is automatically unset as the default. Conversely, if you unset a software image as the default, the other image is automatically set as the default.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the software image is located.

**-image** {image1|image2|remote} - Image Name

This specifies the software image that is to be set or unset as the default.

**[-isdefault** {true|false}] - Is Default Image

This optionally specifies whether the specified image is the default.

**[-force-setdefault** [true]] - Force Setting Image as Default (privilege: advanced)

Force the image to be the default even if the image is not valid.

### Examples

The following example sets the software image named image2 as the default image on a node named node0.

```
node::> system node image modify -node node0 -image image2 -isdefault true
Default Image Changed.
```

## system node image show-update-progress

Show progress information for a currently running update

---

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system node image show-update-progress` command displays the progress of a software-image update initiated by using the `system node image update` command. The command displays progress until the update completes; you can also interrupt it by pressing Ctrl-C.

## Parameters

**-node** {<nodename>|local} - Node

This optionally specifies the name of a node whose image-update progress is to be displayed.

**[-follow [true]]** - Follow the Progress in the Foreground

Do not use background processing for this command. If you do not use this parameter, the value is true.

## Examples

The following example displays image-update progress:

```
node::> system node image show-update-progress
ERROR: command failed: There is no update/install in progress
```

## See Also

`system node image update`

---

## system node image show

Display software image information

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node image show` command displays information about software images. By default, the command displays the following information:

- Node name
- Image name
- Whether the image is the default image
- Whether the image is the current image
- Software version
- Installation date

To display detailed information about a specific software image, run the command with the `-node` and `-image` parameters. The detailed view adds information about the kernel image path, and the root file system image path.

You can specify additional parameters to select specific information. For example, to display information only about software images that are currently running, run the command with the `-iscurrent true` parameter.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node** {<nodename>|local}] - Node

---

Selects information about the software images on the specified node. If this parameter and the `-image` parameter are both used, the command displays detailed information about the specified software image.

**`[-image {image1|image2|remote}]`** - Image Name

Selects information about the software images that match the specified name. If this parameter and the `-node` parameter are specified, the command displays detailed information about the specified software image.

**`[-isdefault {true|false}]`** - Is Default Image

Selects information about the software images with the specified default setting.

**`[-iscurrent {true|false}]`** - Is Current Image

Selects information about the software images that have the specified currency value.

**`[-kernel-path <text>]`** - Kernel Image Path

Selects information about the software images that have the specified kernel image path.

**`[-rootfs-path <text>]`** - Root Filesystem Image Path

Selects information about the software images that have the specified root file system image path.

**`[-version <text>]`** - Software Version

Selects information about the software images that have the specified root file system image path.

**`[-installdate <MM/DD/YYYY HH:MM:SS>]`** - Install Date

Selects information about the software image that have the specified installation date. Specify the date in the format `MM/DD/YYYY HH:MM:SS` [`+- HH:MM`].

## Examples

The following example displays information about the software images on a node named `node1`:

```
cluster1::> system node image show -node node1
Node   Image   Is Default   Is Current   Version   Date
-----
node1
  image1 true      true       8.0         8/20/2009 17:42:42
  image2 false     false      8.0         6/26/2009 17:44:50
2 entries were displayed.
```

---

## system node image update

Perform software image upgrade/downgrade

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node image update` command downloads the software image from a specified location and updates the alternate software image (that is, the image that is not currently running on the node).

At the advanced privilege level, you can specify whether to disable version-compatibility checking.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the software image is located.

**-package** <text> - Package URL

This specifies the location from which the software image is to be downloaded. The location can be specified in any of the following ways:

- As an HTTP URL in the form `http://host_name[:port]/path_to_file`. For instance, `http://example.com/downloads/image.tgz`. The management utility prompts you for a user name and password before beginning the download.

Note:

If you use HTTP to transfer software images, be aware that the management utility does not check whether the Web server is password protected; if it is not, press Enter at the prompt for user name and password.

- As an FTP URL in the form `ftp://host_name[:port]/path_to_file`. For instance, `ftp://example.com/downloads/image.tgz`. If required, the management utility prompts you for a user name and password before beginning the download.
- As a TFTP URL in the form `tftp://host_name[:port]/path_to_file`. For example, `tftp://example.com/downloads/image.tgz`. TFTP does not require a user name or password.

- 
- As a filename of a package left behind by a previous installation, or a package fetched using `system node image get`. For example, `image.tgz`. Available packages can be displayed using `system node image package show`.
  - As a path to a package in a mounted file system in the form `file://localhost/path_to_file`. For example, `file://localhost/mroot/etc/software/image.tgz`.

**`[-replace {image1|image2}]` - Image to Replace**

This optionally specifies the image that is to be replaced when the node is booted from the network.

**`[-setdefault [true]]` - Set Newly Updated Image as Default**

This optionally specifies whether to set the newly updated image as the default image (that is, the image that runs the next time the node is restarted). Note that for this parameter to work correctly, the cluster must be in quorum when the image is updated.

**`[-replace-package [true]]` - Replace the Local File**

Specifies whether an existing package is deleted and replaced with a new package. If this command is entered without using this parameter, its effective value is false and an existing package is not replaced with the new one. If this parameter is used without a value, it is set to true and an existing package is replaced with the new one.

**`[-rename-package <text>]` - Rename the File**

Use this parameter to enter a package name that is different than the file name in the URL.

**`[-background [true]]` - Run in the Background**

This parameter will allow the operation to run in the background. The progress of the operation can be checked with the command `system node image show-update-progress`. If this command is entered without using this parameter, its effective value is false and the operation will run in the foreground. If this parameter is used without a value, it is set to true.

## Examples

The following example updates the software image on a node named `node0` from a software package located at `ftp://ftp.example.com/downloads/image.tgz`:

```
node::> system node image update -node node0 -package ftp://ftp.example.com/
downloads/image.tgz -setdefault true
```

## See Also

---

system node image get   system node image package show   system node image show-  
update-progress

---

## system node image package delete

Delete a software package

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The delete command will delete the specified software package.

### Parameters

**-node** {<nodename>|local} - Node

The package will be deleted from the repository belonging to the node specified with this parameter. The local node is used as the default if this parameter is omitted.

**-package** <text> - Package File Name

This parameter specifies the package to be deleted.

### Examples

```
::> system image package delete image.tgz
1 entry was deleted.
```

## system node image package show

Display software package information

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The package show command displays details of the software packages residing on the storage controller.

### Parameters

{ [-fields <fieldname>, ...]



---

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Selects which node's packages are displayed. The local node is the default if this parameter is omitted.

**[-package <text>]** - Package File Name

This parameter specifies which package's information will be displayed.

## Examples

The following example displays information about software packages:

```
cluster1::> system node image package show    Package
Node Repository Package File Name
-----
node-01
  mroot
      image.tgz
1 entries were displayed.
```

---

## system node platform ifswitch stat

Show Marvell 88E6061 Ethernet switch statistics

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The command `system node platform ifswitch stat` displays the statistics for the Marvell 88E6061 Ethernet switch.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

When provided, the `-node` parameter specifies the nodes for which the Marvell 88E6061 Ethernet switch statistics are to be displayed. When the `-node` parameter is not provided, the command is applied to all the nodes in the cluster.

[-port {sw-RJ45|sw-RLM|sw-PartnerSwitch|sw-e0M}] - Port

This parameter specifies the port for which the statistics are to be displayed.

[-rx-good <integer>] - Rx Good Frames

This parameter specifies the number of good frames received.

[-rx-bad <integer>] - Rx Bad Frames

This parameter specifies the number of bad frames received.

[-rx-discards <integer>] - Rx Discards

This parameter specifies the number of discarded frames.

[-rx-filtered <integer>] - Rx Filtered

This parameter specifies the number of frames that have been filtered.

**[-tx-frames <integer>]** - Tx Frames

This parameter specifies the number of frames transmitted.

**[-tx-collisions <integer>]** - Tx Collisions

This parameter specifies the number of collisions that occurred while transmitting.

**[-status {down|up}]** - Link Status

This parameter specifies the status of the switch link.

**[-media <text>]** - Media

This parameter specifies the status of the transmission media.

### Examples

```
cluster1::*> system node platform ifswitch stat #node cluster1
              Rx Good Frames    Rx Bad Frames
              Tx Frames          Tx Collisions
Node          Port              Rx Discards    Rx Filtered
-----
cluster1
sw-RJ45       49661  9046      0      -      -      -      up auto-100tx-fd
sw-RLM        36197  56475     0      -      -      -      up auto-100tx-fd
sw-PartnerSwitch
              2694   1356      0      -      -      -      up auto-100tx-fd
sw-e0M        45837  52131     0      -      -      -      up auto-100tx-fd
4 entries were displayed.
```

---

## system node platform ifswitch mode modify

Modify the statistics collection mode

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The command `system node platform ifswitch mode show` allows the user to set the status of the statistics collection mode of the Marvell 88E6061 Ethernet switch.

### Parameters

**-node** {<nodename>|local} - Node

When provided, the `-node` parameter specifies the nodes for which the statistics collection mode status is to be set. When the `-node` parameter is not provided, the command is applied to all the nodes in the cluster.

**[-mode** {normal|error}] - Mode

This parameter specifies the status to be set for the statistics collection mode of Marvell 88E6061 Ethernet switch.

### Examples

```
cluster1::*> system node platform ifswitch mode modify -node cluster1 -mode
normal
cluster1::*>
```

### See Also

`system node platform ifswitch mode show`

---

## system node platform ifswitch mode show

Show the statistics collection mode

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The command `system node platform ifswitch mode show` describes the status of the statistics collection mode of the Marvell 88E6061 Ethernet switch.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Selects nodes with the specified node name. When the `-node` parameter is not provided, the command is applied to all the nodes in the cluster.

**[-mode {normal|error}]** - Mode

Selects nodes with the specified status.

### Examples

```
cluster1::*> system node platform ifswitch mode show -node cluster1
Node      Mode
-----
cluster1  normal
```

## system node root-mount create

Create a mount from one node to another node's root volume.

---

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

**Description**

The `system node root-mount create` command produces a root-mount from one node in the cluster to another node's root volume. The root-mount is marked for immediate creation by a background task. Use the `system node root-mount show` command to view the current status of root-mount or verify task completion.

**Parameters**

**-node** <nodename> - Owner of the Root-mount

The node name where the root-mount will be created.

**-root-node** <nodename> - Root-mount Destination Node

The node name that the root-mount will access.

**Examples**

The following example shows the creation of a root-mount from `cluster1::nodeA` to `cluster1::nodeB` and the verification of the successful completion.

```
cluster1::> system node root-mount show
This table is currently empty.

cluster1::> system node root-mount create -node nodeA -root-node nodeB

cluster1::> system node root-mount show
Node          Root Node      State      Last Error
-----
nodeA         nodeB          ready
```

**See Also**

`system node root-mount show`   `system node root-mount delete`

---

# system node root-mount delete

Delete a mount from one node to another node's root volume.

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system node root-mount delete` command removes a root-mount from one node in the cluster to another node's root volume. The root-mount is marked for immediate deletion by a background task. Use the `system node root-mount show` command to view the current status of root-mount or verify task completion.

## Parameters

**-node** <nodename> - Owner of the Root-mount

The node which has the mount.

**-root-node** <nodename> - Root-mount Destination Node

The node accessed by the mount.

## Examples

This example shows the deletion of a root-mount from `cluster::nodeA` to `cluster::nodeB` and the verification of the command's successful completion.

```
cluster1::> system node root-mount show
Node      Root Node      State      Last Error
-----
nodeA      NodeB                  ready
cluster1::> system node root-mount delete -node nodeA -root-node nodeB
cluster1::> system node root-mount show
This table is currently empty.
```

## See Also

`system node root-mount show`   `system node root-mount create`

---

## system node root-mount show

Show the existing mounts from any node to another node's root volume.

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node root-mount show` command displays the status of current root-mounts from any node to another node's root volume. These root-mounts are used by cluster services to access data on other nodes in the cluster. These root-mounts are not pre-created, but are created as they are needed. They can also be manually created or deleted.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node <nodename>]** - Owner of the Root-mount

Selects information about root-mounts that exist on the specified node.

**[-root-node <nodename>]** - Root-mount Destination Node

Selects information about root-mounts that connect to the specified node.

**[-create-time <MM/DD/YYYY HH:MM:SS>]** - Mount Creation Time

Selects information about root-mounts that were created at the specified time.

**[-state <Mount State>]** - State of the Root-Mount

Selects information about root-mounts that have the specified state. The states are:

- unknown: The state of the root-mount is being determined.
- initializing: A root-mount was found and needs testing to determine the correct state.



- **mount-requested:** The root-mount has been requested, but is not ready.
- **mounting:** The root-mount is being created, but is not ready.
- **ready:** The root-mount is ready to be used.
- **not-responding:** The root-mount exists but is not responding.
- **does-not-exist:** No root-mount is possible to this node's root volume.
- **ha-busy:** The root-mount is busy pending completion of an HA event.
- **clean-up-requested:** The root-mount is being deleted.
- **cleaning-up:** The root-mount is being deleted.
- **create-error:** The root-mount could not be created.

**[-last-error <text>]** - Last Error

Selects information about root-mounts that have the specified last-error value.

### Examples

The following example shows the default state of the root-mounts on a cluster that is not using root-node services:

```
cluster1::> system node root-mount show
This table is currently empty.
```

The following example displays the root-mounts that exist for a cluster that has nodeA mounted to nodeB, and nodeB mounted to nodeA:

```
cluster1::> system node root-mount show
Node          Root Node      State      Last Error
-----
nodeA          nodeB          ready
nodeB          nodeA          ready
2 entries were displayed.
```

## HA Considerations

When a node in the cluster is taken over by its partner node, all root-mounts to that node will be automatically deleted. Any active root-mounts will be recreated to access the root volume now located on the partner node.

### See Also

`system node root-mount create`   `system node root-mount delete`

---

## system node service-processor reboot-sp

Reboot the Service Processor on a node

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor reboot-sp` command reboots the Service Processor of the specified node.

This command does not currently support Remote LAN Module (RLM).

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node whose Service Processor is to be rebooted.

**[-image** {primary|backup}] - Image to Boot with After Reboot

This parameter specifies the image that Service Processor uses after the reboot. By default, the `primary` image is used.

### Examples

The following command reboots the Service Processor of node "node1" into the `primary` image.

```
cluster1::> system node service-processor reboot-sp -node node1 -image primary
NOTE : If your console connection is through the SP, it will be disconnected.
Do you want to reboot the SP ? {y|n}: y
cluster1::>
```

The following command reboots the Service Processors of all nodes. Since `-image` is not specified, the Service Processors will boot into the `primary` image.

```
cluster1::> system node service-processor reboot-sp -node *
NOTE : If your console connection is through the SP, it will be disconnected.
Do you want to reboot the SP ? {y|n}: y
2 entries were acted on.
cluster1::>
```

---

## system node service-processor show

Display the Service Processor information

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor show` command displays information about the Service Processor of each node in a cluster. You can limit output to specific types of information and specific nodes in the cluster, or filter output by specific field values.

In case a node is offline or its Service Processor management daemon is down, the command displays the last known IP address of its Service Processor. Only the IP address is displayed in such cases.

This command does not currently support Remote LAN Module (RLM) completely. If you run this command on nodes that use RLM, the output displays RLM as the type and - for all other fields.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**node** {<nodename>|local}] - Node

Selects information for the Service Processor of the specified node.

[-**type** {RLM|SP}] - Type of Device

Selects information for the Service Processors of the specified type.

[-**status** {online|offline|sp-daemon-offline|node-offline|degraded|rebooting|unknown}] - Status

Selects information for the Service Processors whose status matches the specified value.

---

**[-ip-configured {true|false}]** - Is Network Configured

Selects information for the Service Processors whose network is configured (`true`) or not configured (`false`).

**[-address <IP Address>, ...]** - Public IP Address

Selects information for the Service Processors that use the specified IP address or addresses.

**[-mac <MAC Address>]** - MAC Address

Selects information for the Service Processors that use the specified MAC address.

**[-fw-version <text>]** - Firmware Version

Selects information for the Service Processors that are running the specified firmware version.

**[-part-num <text>]** - Part Number

Selects information for the Service Processors that have the specified part number.

**[-serial-num <text>]** - Serial Number

Selects information for the Service Processors that have the specified serial number.

**[-ipmi-ver <text>]** - IPMI Version

Selects information for the Service Processors that have the specified Intelligent Platform Management Interface version.

**[-dev-rev <text>]** - Device Revision

Selects information for the Service Processors that have the specified device revision.

**[-autoupdate-enabled {true|false}]** - Is Firmware Autoupdate Enabled

Selects information for the Service Processors that have the specified status for firmware automatic update.

## Examples

The following example displays basic information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor show
Node          Type Status      IP          Firmware
-----      -
node1         SP   online    true        2.2X5
node2         SP   online    true        2.2X5
2 entries were displayed.
cluster1::>
```

---

The following example displays all available information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor show -instance
```

```

      Node: node1
      Type of Device: SP
      Status: online
Is Network Configured: true
      Public IP Address: 192.168.1.201
      MAC Address: ab:cd:ef:fe:ed:01
      Firmware Version: 2.2X5
      Part Number: Not Applicable
      Serial Number: Not Applicable
      IPMI Version: 2.0
      Device Revision: Not Applicable
Is Firmware Autoupdate Enabled: true
Is New Firmware Available: false
      New Firmware Version: 0.0.0
```

```

      Node: node2
      Type of Device: SP
      Status: online
Is Network Configured: true
      Public IP Address: 192.168.1.202
      MAC Address: ab:cd:ef:fe:ed:02
      Firmware Version: 2.2X5
      Part Number: Not Applicable
      Serial Number: Not Applicable
      IPMI Version: 2.0
      Device Revision: Not Applicable
Is Firmware Autoupdate Enabled: true
Is New Firmware Available: false
      New Firmware Version: 0.0.0
```

```
2 entries were displayed.
```

```
cluster1::>
```

The following example displays only the type, status, firmware version, and Intelligent Platform Management Interface (IPMI) version for the Service Processors of all the nodes.

```
cluster1::> system node service-processor show -fields type,status,fw-  
version,ipmi-ver
```

```
node      type status fw-version ipmi-ver  
-----  
node1     SP   online 2.2X5      2.0  
node2     SP   online 2.2X5      2.0  
2 entries were displayed.
```

```
cluster1::>
```

---

## system node service-processor image modify

Enable/Disable automatic firmware update

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor image modify` command enables or disables automatic firmware update on the Service Processor of specified node or nodes.

This command does not currently support Remote LAN Module (RLM).

### Parameters

**-node** {<nodename>|local} - Node

The parameter specifies the node on which automatic Service Processor firmware update is to be enabled or disabled.

**[-autoupdate** {true|false}] - Firmware Autoupdate

Setting this parameter to `true` enables automatic firmware update. Setting this parameter to `false` disables automatic firmware update. This is a mandatory parameter.

### Examples

The following command enables automatic firmware update for Service Processor on the local node.

```
cluster1::> system node service-processor image modify -node local -autoupdate
true
cluster1::>
```

The following command enables automatic firmware update for Service Processors on all the nodes.

```
cluster1::> system node service-processor image modify -node * -autoupdate true
2 entries were modified.
cluster1::>
```

---

## system node service-processor image show

Display the details of currently installed Service Processor firmware image

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor image show` command displays information about the currently installed firmware images on the Service Processor of each node in a cluster. You can limit output to specific types of information and specific nodes in the cluster, or filter output by specific field values.

This command does not currently support Remote LAN Module (RLM) completely. If you run this command on nodes that use RLM, the output displays RLM as the type and - for all other fields.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

Selects firmware image information for the Service Processor of the specified node.

[-image {primary|backup}] - Image

Selects firmware image information for the Service Processors that are running the primary or backup image as specified.

[-type {RLM|SP}] - Type

Selects firmware image information for the Service Processors of the specified type.

[-status {installed|corrupt|updating|auto-updating|none}] - Image Status

---

Selects firmware image information for the Service Processors whose image status matches the specified value.

**[-is-current {true|false}]** - Is Image Current

Selects firmware image information for the Service Processors whose current image matches the specified status.

**[-version <text>]** - Firmware Version

Selects firmware image information for the Service Processors running the specified firmware version.

**[-autoupdate {true|false}]** - Firmware Autoupdate

Selects firmware image information for the Service Processors whose automatic update matches the specified configuration.

**[-last-update-status {failed|passed}]** - Last Update Status

Selects firmware image information for the Service Processors whose last update is of the specified status.

## Examples

The following command displays basic firmware information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor image show
Node           Type  Image  Status  Is Current Version
-----
node1          SP   primary installed true   2.2X8
              SP   backup  installed false  2.2X5
node2          SP   primary installed true   2.2X8
              SP   backup  installed false  2.2X5
4 entries were displayed.
cluster1::>
```

The following command displays all available firmware information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor image show -instance
Node: node1
Image: primary
Type: SP
Image Status: installed
Is Image Current: true
Firmware Version: 2.2X8
Firmware Autoupdate: true
Last Update Status: passed

Node: node1
Image: backup
Type: SP
Image Status: installed
Is Image Current: false
Firmware Version: 2.2X5
Firmware Autoupdate: true
```



---

```
Last Update Status: passed
      Node: node2
      Image: primary
      Type: SP
      Image Status: installed
      Is Image Current: true
      Firmware Version: 2.2X8
      Firmware Autoupdate: true
      Last Update Status: passed

      Node: node2
      Image: backup
      Type: SP
      Image Status: installed
      Is Image Current: false
      Firmware Version: 2.2X5
      Firmware Autoupdate: true
      Last Update Status: passed
4 entries were displayed.

cluster1::>
```

---

## system node service-processor image update

Update Service Processor firmware

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor image update` command installs a new firmware version on the Service Processor of specified node in a cluster. This command also specifies which firmware image is installed on the Service Processor and how.

You can use the command `system node service-processor image update-progress show` to check the progress of the update.

This command does not currently support Remote LAN Module (RLM).

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node whose Service Processor's firmware is to be updated.

**[-package <text>]** - Firmware Package

This parameter specifies the package that will be installed. You can find the package file in the SP Update Repository field of the `system node image package show` command. If you do not specify this parameter, the Service Processor is updated to the most recent version of the firmware that is available in the update repository. You must specify this parameter if `baseline` is false or omitted.

**[-baseline {true|false}]** - Install Baseline

If you set this parameter to true, the command installs the Service Processor firmware version that is bundled with the currently running release of Data ONTAP. This is a safety mechanism that allows you to revert the SP firmware to the version that was qualified and bundled with the currently running version of Data ONTAP on your system. If not specified, this parameter defaults to false.

**-update-type** {full|differential} - Type

This parameter specifies the type of upgrade to be performed. If you set the value to `full`, the entire firmware image is updated on the Service Processor. If you set the

---

value to `differential`, only the changed portions of the firmware image are updated on the Service Processor.

**`[-clear-logs {true|false}]` - Clear Logs After Update**

If you set this parameter to `true`, the command resets log settings to factory default and clears contents of all logs maintained by the Service Processor, including:

- Event logs
- IPMI logs
- Forensics logs

## Examples

The following command reverts the firmware on the Service Processor of the local node to the version that was packaged with the currently running release of Data ONTAP. A complete install will be performed, clearing all logs maintained by the Service Processor. The second command displays the status of the firmware install in progress.

```
cluster1::> system node service-processor image update -node local -update-type
full -baseline true -clear-logs true
cluster1::>
cluster1::> system node service-processor image update-progress show
Node           In      Start Time          Percent
----- Progress ----- Done      End Time -----
node1          yes      8/28/2012 20:00:34    99
node2          no       -                    0
2 entries were displayed.
cluster1::>
```

## See Also

`system node image package show`   `system node service-processor image update-progress show`

---

## system node service-processor image update-progress show

Display status for the latest Service Processor firmware update

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor image update-progress show` command displays the progress information of firmware updates on the Service Processor of the specified nodes. The "In-Progress" field displays "no" if no update is in progress.

This command does not currently support Remote LAN Module (RLM) completely. If you run this command on nodes that use RLM, the output will always display "no" for the "In-Progress" field.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

This parameter displays the status of Service Processor firmware update for the specified node.

**[-start-time <MM/DD/YYYY HH:MM:SS>]** - Latest SP Firmware Update Start Timestamp

This parameter displays the status of the Service Processor whose firmware update start time matches the specified value.

**[-percent-done <integer>]** - Latest SP Firmware Update Percentage Done

---

This parameter displays the status of the Service Processor whose update completion percentage matches the specified value.

**[-end-time <MM/DD/YYYY HH:MM:SS>]** - Latest SP Firmware Update End Timestamp

This parameter displays the status of the Service Processor whose firmware update end time matches the specified value.

**[-in-progress {yes|no}]** - Is Update in Progress

This parameter displays the update status of the Service Processor that matches the specified in-progress status.

## Examples

The following example starts a firmware update on the local node and then uses the command `system node service-processor image update-progress show` to display progress of firmware updates on Service Processors of all nodes in the system.

```
cluster1::> system node service-processor image update -node local -update-type
full -baseline true -clear-logs true
cluster1::>
cluster1::> system node service-processor image update-progress show
Node           In      Progress Start Time           Percent      End Time
-----
node1          yes      8/28/2012 20:00:34  99
node2          no      -                  0
2 entries were displayed.
cluster1::>
```

---

## system node service-processor network modify

Modify the network configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor network modify` command modifies the network configuration of the Service Processor of specified node or nodes in a cluster.

This command does not currently support Remote LAN Module (RLM).

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node whose Service Processor's network configuration is to be modified.

**-address-type** {IPv4|IPv6} - Address Type

This parameter specifies whether the IPv4 or the IPv6 configuration is to be modified.

**[-enable** {true|false}] - Interface Enabled

This parameter enables or disables the underlying network interface for the specified `address-type`. This is a mandatory parameter.

**[-dhcp** {v4|none}] - DHCP Status

If this parameter is set to `v4`, the Service Processor uses network configuration from the DHCP server. Otherwise, the Service Processor uses the network address you specify. If this parameter is not set to `v4` or is not specified, you must specify the IP address, netmask, prefix-length, and gateway in the command. DHCP is not supported for IPv6 configuration.

**[-ip-address** <IP Address>] - IP Address

This parameter specifies the public IP address for the Service Processor. You must specify this parameter when the `-dhcp` parameter is not set to `v4`.

**[-netmask** <IP Address>] - Netmask

---

This parameter specifies the netmask for a Service Processor that uses an IPv4 address. This parameter has no effect if the IP address type is set to IPv6. You must specify this parameter when DHCP is not v4 and the address type is IPv4.

**[-prefix-length <integer>]** - Prefix Length of Subnet Mask

This parameter specifies the network prefix-length of the Service Processor if the address type is set to IPv6. The parameter has no effect when the address type is set to IPv4. You must specify this parameter when DHCP is not set to v4 and when the address type is set to IPv6.

**[-gateway <IP Address>]** - Gateway IP Address

This parameter specifies network gateway of the Service Processor. You must specify this parameter when DHCP is not set to v4.

## Examples

The following example enables the network interface for IPv4 on the Service Processor of the local node. It first displays the current network configuration information of the local node to show the network interface is initially disabled, and then enables it with IP address 192.168.1.202, netmask as 255.255.255.0 and gateway as 192.168.1.1. It finally displays the network configuration again to confirm the specified values took effect.

```
cluster1::> system node service-processor network show -instance -node local
      Node: node2
      Address Type: IPv4
      Interface Enabled: false
      Type of Device: SP
      Status: online
      Link Status: disabled
      DHCP Status: -
      IP Address: -
      MAC Address: ab:cd:ef:fe:ed:02
      Netmask: -
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: -

      Node: node2
      Address Type: IPv6
      Interface Enabled: false
      Type of Device: SP
      Status: online
      Link Status: disabled
      DHCP Status: none
      IP Address: -
      MAC Address: ab:cd:ef:fe:ed:02
      Netmask: -
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: -
2 entries were displayed.

cluster1::>

cluster1::> system node service-processor network modify -node local -address-
type IPv4 -enable true -ip-address 192.168.1.202 -netmask 255.255.255.0 -gateway
192.168.1.1
```

---

```
cluster1::>
cluster1::> system node service-processor network show -instance -node local
      Node: node2
      Address Type: IPv4
      Interface Enabled: true
      Type of Device: SP
      Status: online
      Link Status: up
      DHCP Status: none
      IP Address: 192.168.1.202
      MAC Address: ab:cd:ef:fe:ed:02
      Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.1.1

      Node: node2
      Address Type: IPv6
      Interface Enabled: false
      Type of Device: SP
      Status: online
      Link Status: disabled
      DHCP Status: none
      IP Address: -
      MAC Address: ab:cd:ef:fe:ed:02
      Netmask: -
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: -
2 entries were displayed.
cluster1::>
```



---

## system node service-processor network show

Display the network configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system node service-processor network show` command displays the network configuration of the Service Processor of each node in a cluster. You can limit output to specific types of information and specific nodes in the cluster, or filter output by specific field values.

In case a node is offline or its Service Processor management daemon is down, the command displays the last known IP address of its Service Processor. Only the IP address is displayed in such cases.

This command does not currently support Remote LAN Module (RLM) completely. If you run this command on nodes that use RLM, the output displays RLM as the type and - for all other fields.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Selects network configuration information for the Service Processor of the specified node.

**[-address-type {IPv4|IPv6}]** - Address Type

Selects network configuration information for the Service Processors that have the specified IP address type.

**[-enable {true|false}]** - Interface Enabled

---

Selects network configuration information for the Service Processors whose network interface for the given `address-type` is enabled or disabled as specified.

**[-type {RLM|SP}]** - Type of Device

Selects network configuration information for the Service Processors of the specified type.

**[-status {online|offline|sp-daemon-offline|node-offline|degraded|rebooting|unknown}]** - Status

Selects network configuration information for the Service Processors whose status matches the specified value.

**[-link-status {up|down|disabled|unknown}]** - Link Status

Selects network configuration information for the Service Processors whose link status matches the specified value.

**[-dhcp {v4|none}]** - DHCP Status

Selects network configuration information for the Service Processors whose DHCP status matches the specified value.

**[-ip-address <IP Address>]** - IP Address

Selects network configuration information for the Service Processors that use the specified IP address.

**[-mac <MAC Address>]** - MAC Address

Selects network configuration information for the Service Processors that use the specified MAC address.

**[-netmask <IP Address>]** - Netmask

This parameter displays information only for the Service Processors that use the specified netmask.

**[-prefix-length <integer>]** - Prefix Length of Subnet Mask

Selects network configuration information for the Service Processors whose prefix length of subnet mask matches the specified value.

**[-router-ip <IP Address>]** - Router Assigned IP Address

Selects network configuration information for the Service Processors whose router-assigned IP address matches the specified value.

**[-link-local-ip <IP Address>]** - Link Local IP Address

Selects network configuration information for the Service Processors whose link local IP address matches the specified value.

**[-gateway <IP Address>]** - Gateway IP Address

Selects network configuration information for the Service Processors whose gateway IP address matches the specified value.

## Examples

The following example displays basic network configuration information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor network show
Node           Status      Address Type      Link State IP Address
-----
node1          online      IPv4      up          192.168.1.201
                DHCP: v4
                MAC Address: ab:cd:ef:fe:ed:01
                Network Gateway: 192.168.1.1
                Network Mask (IPv4 only): 255.255.255.0
                Prefix Length (IPv6 only): -

node1          online      IPv6      disabled   -
                DHCP: none
                MAC Address: ab:cd:ef:fe:ed:01
                Network Gateway: -
                Network Mask (IPv4 only): -
                Prefix Length (IPv6 only): -

node2          online      IPv4      up          192.168.1.202
                DHCP: v4
                MAC Address: ab:cd:ef:fe:ed:02
                Network Gateway: 192.168.1.1
                Network Mask (IPv4 only): 255.255.255.0
                Prefix Length (IPv6 only): -

node2          online      IPv6      disabled   -
                DHCP: none
                MAC Address: ab:cd:ef:fe:ed:02
                Network Gateway: -
                Network Mask (IPv4 only): -
                Prefix Length (IPv6 only): -

4 entries were displayed.
cluster1::>
```

The following example displays all available network configuration information for the Service Processors of all the nodes.

```
cluster1::> system node service-processor network show -instance
Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: v4
IP Address: 192.168.1.201
MAC Address: ab:cd:ef:fe:ed:01
```

---

```

                                Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.1.1

                                Node: node1
                                Address Type: IPv6
Interface Enabled: false
Type of Device: SP
                                Status: online
                                Link Status: disabled
                                DHCP Status: none
                                IP Address: -
                                MAC Address: ab:cd:ef:fe:ed:01
                                Netmask: -
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: -

                                Node: node2
                                Address Type: IPv4
Interface Enabled: true
Type of Device: SP
                                Status: online
                                Link Status: up
                                DHCP Status: v4
                                IP Address: 192.168.1.202
                                MAC Address: ab:cd:ef:fe:ed:02
                                Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.1.1

                                Node: node2
                                Address Type: IPv6
Interface Enabled: false
Type of Device: SP
                                Status: online
                                Link Status: disabled
                                DHCP Status: none
                                IP Address: -
                                MAC Address: ab:cd:ef:fe:ed:02
                                Netmask: -
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: -
4 entries were displayed.
cluster1::>

```

---

## system node upgrade-revert show

Display upgrade/revert node status.

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system node upgrade-revert show` command displays information about the status of upgrades or reversions. If an upgrade has failed, this command enables you to determine which phase of the upgrade contains the failed upgrade task and the reason for the failure.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Use this parameter to display status information only about upgrades or reversions that are slated to occur on the nodes you specify.

**[-upgrade-version <integer>]** - Cluster Upgrade Version

Selects status information about upgrades or reversions that are to the version number you specify.

**[-startup-phase {pre-root|pre-apps|post-apps}]** - Startup Phase

Selects status information about upgrades or reversions that are slated to occur during the startup phase you specify. Startup phases are:

- `pre-root` - Upgrade is applied before `mroot` is mounted
- `pre-apps` - Upgrade is applied before other cluster apps are started
- `post-apps` - Upgrade is applied after all RDB apps are online

---

**[-status <Upgrade/Revert Execution Status>]** - Execution Status

Selects status information about upgrades or reversions that have the execution status you specify. Execution statuses are:

- prepared - Ready to upgrade
- applied - Successful upgrade
- reverted - Successful reversion
- failed - Unsuccessful upgrade or reversion
- aborted - Unsuccessful upgrade or reversion
- skipped - Upgrade or reversion was skipped for that phase
- locked - Upgrading or reverting

**[-status-msg <text>]** - Status Message

Selects status information about upgrades or reversions that have the status message you specify. The status message displays the current status of the phase with which it appears.

**[-direction {upgrade|revert}]** - Upgrade/Revert Direction

Use this parameter with the value `upgrade` to select status information about upgrades. Use this parameter with the value `revert` to select status information about reversions.

**[-node-status {reverting|complete|not-needed|aborted|failed|waiting|in-progress|stopped}]** - Node Status

Selects status information about upgrades or reversions that have the status you specify on nodes where they are slated to occur. Node statuses are:

- aborted - Upgrade process aborted. Contact support personnel.
- failed - Upgrade process failed. Contact support personnel.
- stopped - Upgrade process stopped due to node or management application restart. Use the `system node upgrade-revert upgrade` command to complete the upgrade manually.
- complete - Upgrade process completed successfully.
- waiting - Upgrade process is waiting the replication database to come online or for applications to be stable. If the RDB is not online, check network connectivity using `cluster show` and `cluster ping-cluster` to ensure that all nodes are healthy and in communication.

---

**[`-node-status-msg` <text>] - Node Status Message**

Selects status information about upgrades or reversions that have the node status message you specify. The node status message displays the upgrade or reversion status of the node with which it appears. If the upgrade or reversion fails, this message provides information that helps to diagnose the cause of the failure.

**Examples**

The following example shows typical output for a cluster with two nodes. Status messages for each phase display information about the the tasks in that phase.

```
cluster1::*> system node upgrade-revert show
Node: node1                                     Status: complete
Status Message: The upgrade is complete.

Vers Phase      Status  Upgrade Phase Status Message
-----
200 pre-root    applied No upgrade is required for this phase.
200 pre-apps    applied Upgrade successful.
200 post-apps   applied Upgrade successful.

Node: node2                                     Status: complete
Status Message: The upgrade is complete.

Vers Phase      Status  Upgrade Phase Status Message
-----
200 pre-root    applied No upgrade is required for this phase.
200 pre-apps    applied Upgrade successful.
200 post-apps   applied Upgrade successful.
6 entries were displayed.
```

**See Also**

`system node upgrade-revert upgrade`   `cluster show`   `cluster ping-cluster`

---

## system node upgrade-revert upgrade

Run the upgrade at a specific phase.

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system node upgrade-revert upgrade` command manually executes an upgrade. Use this command to execute an upgrade after issues that caused an upgrade failure are resolved. If the upgrade is successful, no messages display.

Before the command executes upgrades, it checks the configuration of the nodes in the cluster. If no upgrades are needed, the command displays a message and does not execute any upgrades.

### Parameters

None

### Examples

This example shows command output if node configuration is current.

```
cluster1::*> system node upgrade-revert upgrade
The node configuration is up-to-date. No upgrade is needed.
```

## system script delete

Delete saved CLI session logs

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system script delete` command deletes files that contain CLI session records. Use the `system script show` command to display saved CLI sessions.

### Parameters

**-username <text>** - Log Owner Username



---

Use this parameter to specify the name of the user whose CLI session record files are deleted. The default is the username is that of the logged in user.

**-filename** <text> - Log Filename

Use this parameter to specify the names of CLI session record files to delete.

## Examples

The following example shows how to delete the files named `sessionlog2` and `sessionlog3`.

```
cluster1::> system script delete -filename sessionlog2,sessionlog3
```

The following example deletes all saved script files.

```
cluster1::> system script delete *
```

## See Also

`system script show`

---

## system script show

Display saved CLI session logs

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system script show` command displays information about files that contain records of CLI sessions.

For security reasons, the command normally displays only the script files created by the logged in user. Administrative users can display all log files using the `-user` parameter.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-user ]

Use this parameter to display all script files created by all users, along with the username associated with each file.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-username <text>] - Log Owner Username

Use this parameter to display information only about files saved by the user you specify. The default username is that of the logged in user.

[-filename <text>] - Log Filename

Use this parameter to display information only about files that have the file name you specify.

[-size-limit {<integer>[KB|MB|GB|TB|PB]] - Logfile Size Limit

Use this parameter to display information only about files that have the size limit you specify.

---

**[-state <State of CLI session log>]** - Current State

Use this parameter to display information only about files that have the state you specify. Valid values for this parameter are `open-and-logging`, `file-full`, and `file-closed`.

**[-size {<integer>[KB|MB|GB|TB|PB]}]** - Current Logfile Size

Use this parameter to display information only about files that are the size you specify.

**[-mtime <MM/DD/YYYY HH:MM:SS>]** - Last Modification Time

Use this parameter to display information only about files that were last modified at the date and time you specify.

**[-this-session {yes|no}]** - Session is Logging

Use this parameter with the value `yes` to display information only about files that are recording the current CLI session. Use this parameter with the value `no` to display information only about files that are not recording the current CLI session.

## Examples

The following example displays typical system script information.

```
cluster1::> system script show
      This
FileName      Sess State      Size      Last Mod Date
-----
sessionlog1   no    file-closed  435B      12/2/2008 10:51:12
sessionlog2   yes   open-and-logging 193B      12/2/2008 10:51:29
2 entries were displayed.
```

---

## system script start

Start logging all CLI I/O to session log

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system script start` command starts creating a record of your CLI session. The record is stored in a file. Use the `system script show -this-session yes` command to display files that are recording the current CLI session. Use the `system script stop` command to stop recording the current CLI session.

### Parameters

**-filename** <text> - Filename to Log To

Use this parameter to specify the file name to which the CLI session record is saved.

**-size-limit** {<integer>[KB|MB|GB|TB|PB]} - Logfile Size Limit Max:2GB

Use this parameter to specify the maximum size of the file that contains the CLI session record. When the file size reaches this limit, recording stops. The default file size limit is 1 MB. The maximum file size limit is 2 GB.

### Examples

The following example shows how to start creating a record of the CLI session in a file named `sessionlog3`. The size limit of this file is 20 MB.

```
cluster1::> system script start -filename sessionlog3 -size-limit 20MB
```

### See Also

`system script show`   `system script stop`

---

## system script stop

Stops logging CLI I/O

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system script stop` command stops creating a record of your CLI session, if you started creating the record by using the `system script start` command. Use the `system script show -this-session yes` command to display files that are recording the current CLI session.

### Parameters

None

### Examples

The following example shows how to stop creating a record of your CLI session.

```
cluster1::> system script stop
```

### See Also

`system script start`   `system script show`

---

## system script upload

Upload the selected CLI session log

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system script upload` command uploads a CLI session record file to a remote location. Specify the remote location using an FTP or HTTP URI. Use the `system script show` command to display saved CLI sessions. Use the `system script start` command to record a CLI session and save it to a file.

### Parameters

**-username** <text> - Username If Not Your Own

Use this parameter to specify the name of the user who owns the file to upload. By default, this is the user who is logged in.

**-filename** <text> - Filename to Log To

Use this parameter to specify the name of a file to be uploaded.

**-destination** {(ftp|http)://(hostname|IPv4 Address|['IPv6 Address'])...} - URI to Send File To

Use this parameter to specify the FTP or HTTP destination of the file.

### Examples

The following example shows how to upload the file named `sessionlog3` to the destination `ftp://now.example.com/cli_sessions`.

```
cluster1::> system script upload -filename sessionlog3 -destination ftp://now.example.com/cli_sessions
```

### See Also

`system script show`   `system script start`

---

## system services firewall modify

Modify firewall status

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall modify` command modifies a node's firewall configuration.

### Parameters

**-node** {<nodename>|local} - Node

Use this parameter to specify the node on which to modify firewall configuration.

**[-enabled** {true|false}] - Service Enabled

Use this parameter to specify whether firewall protection is enabled ("true") or disabled ("false") for the node's network ports. The default setting is `true`.

**[-logging** {true|false}] - Enable Logging

Use this parameter to specify whether logging is enabled ("true") or disabled ("false") for the firewall service. The default setting is `false`.

### Examples

The following example enables firewall protection and logging for a node named node1:

```
cluster1::> system services firewall modify -node node1 -enabled true -logging true
```

## system services firewall show

Show firewall status

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall show` command displays firewall configuration and logging information. If the command is issued without any parameters, it displays

---

information about all nodes in the cluster. You can also query specific nodes for their firewall information by running the command with the `-node` parameter.

## Parameters

**{ [-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}]** - Node

Selects information about the firewall settings on the node you specify.

**[-enabled {true|false}]** - Service Enabled

Selects firmware image information about the nodes with the firewall enabled ("true") or disabled ("false").

**[-logging {true|false}]** - Enable Logging

Selects firmware image information about the nodes with firewall logging enabled ("true") or disabled ("false").

## Examples

The following example displays information about firewall configuration for all nodes in the cluster:

```
cluster1::> system services firewall show
Node      Enabled Logging
-----
node0     true    false
node1     true    false
node2     true    false
node3     true    false
4 entries were displayed.
```



---

## system services firewall policy clone

Clone an existing firewall policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall policy clone` command creates a new firewall policy that is an exact copy of an existing policy, but has a new name.

### Parameters

**-policy** <text> - Firewall Policy to be Cloned

Use this parameter to specify the name of the existing policy to copy.

**-new-policy-name** <text> - Name of New Firewall Policy

Use this parameter to specify the name of the new policy to create.

### Examples

This example creates a new firewall policy named "data2" from an existing firewall policy named "data".

```
cluster1::> system services firewall policy clone -policy data -new-policy-name data2
```

## system services firewall policy create

Create a new firewall policy or add a service to an existing firewall policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall policy create` command creates a firewall policy entry with the specified name and network service. This command is used both to create the first network service associated with a new firewall policy, or to add to an existing firewall policy by associating another network service with an existing policy. You can optionally specify one or more IP addresses with corresponding netmasks that are allowed to use the firewall policy entry.

---

You can use the `network interface modify` command with the `-firewall-policy` parameter to put a firewall policy into effect for a given logical interface by modifying that logical interface to use the specified firewall policy.

## Parameters

**-policy** <text> - Policy Name

Use this parameter to specify the name of the policy that is to be created.

**-service** <service> - Service Name

Use this parameter to specify the network service that is associated with the policy. Possible values include:

- `default` - The default protocol or protocols for the port to which the firewall is applied
- `http` - The HTTP protocol
- `https` - The HTTPS protocol
- `ntp` - The NTP protocol
- `rsh` - The RSH protocol
- `snmp` - The SNMP protocol
- `ssh` - The SSH protocol
- `telnet` - The Telnet protocol

**-action** <fw\_policy\_action> - Pass or Block traffic

Use this parameter to specify whether the firewall should pass ("allow") or block ("deny") network traffic.

**[-ip-list** <IpAddress/Mask>, ...] - IP Address List

Use this parameter to specify one or more IP addresses with corresponding netmasks that are affected by this firewall policy. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25". Multiple address/netmask pairs should be separated with commas. Use the value `0.0.0.0/0` for "any".

## Examples

The following example creates a firewall policy named `data` that uses the SSH protocol and enables access from all IP addresses on the 192.0.2.128/25 subnet:

```
cluster1::> system services firewall policy create -policy data -service ssh -ip-list 192.0.2.128/25 -action allow
```

---

The following example adds an entry to the firewall policy named data, associating the HTTPS protocol with that policy and enabling access from all IP addresses on the 192.0.2.128/25 subnet:

```
cluster1::> system services firewall policy create -policy data -service https -  
ip-list 192.0.2.128/25 -action allow
```

## See Also

network interface modify

---

## system services firewall policy delete

Remove a service from a firewall policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall policy delete` command deletes a firewall policy. You cannot delete a policy that is being used by a logical interface. Use the `network interface modify` command with the `-firewall-policy` parameter to change a network interface's firewall policy.

### Parameters

**-policy** <text> - Policy Name

Use this parameter to specify the name of the policy to delete.

**-service** <service> - Service Name

Use this parameter to specify the policy's network service to delete.

**-action** <fw\_policy\_action> - Pass or Block traffic

Use this parameter to specify the action of the policy to delete.

### Examples

The following example deletes a firewall policy that uses the Telnet protocol on the policy named `data`:

```
cluster1::> system services firewall policy delete -policy data -service telnet
```

Use wildcards to delete entire policies at once, or particular services from every policy. This example deletes the entire intercluster policy.

```
cluster1::> system services firewall policy delete -policy intercluster -service *
```

This example deletes the telnet service from every policy.

```
cluster1::> system services firewall policy delete -policy * -service telnet
```

### See Also

`network interface modify`

---

## system services firewall policy modify

Modify a policy's IP-list

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall modify` command enables you to modify the list of IP addresses and netmasks associated with a firewall policy.

### Parameters

**-policy** <text> - Policy Name

Use this parameter to specify the name of the policy to modify.

**-service** <service> - Service Name

Use this parameter to specify the policy's network service to modify.

**-action** <fw\_policy\_action> - Pass or Block traffic

Use this parameter to specify whether the firewall should pass ("allow") or block ("deny") network traffic.

**[-ip-list** <IpAddress/Mask>, ...] - IP Address List

Use this parameter to specify one or more IP addresses with corresponding netmasks that are affected by this firewall policy. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25". Multiple address/netmask pairs should be separated with commas. Use the value 0.0.0.0/0 for "any".

### Examples

The following example modifies the firewall policy named `data` that uses the SSH protocol to enable access from all addresses on the 192.0.2.128 subnet:

```
cluster1::> system services firewall policy modify -policy data -service ssh -ip-list 192.0.2.128/25 -action allow
```

### See Also

`system services firewall modify`

---

## system services firewall policy show

Show firewall policies

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services firewall policy show` command displays information about firewall policies.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**policy** <text>] - Policy Name

Selects information about the policy you specify.

[-**service** <service>] - Service Name

Selects information about the services you specify.

[-**action** <fw\_policy\_action>] - Pass or Block traffic

Selects information about the firewall policies that match the action you specify.

[-**ip-list** <IpAddress/Mask>, ...] - IP Address List

Selects information about the firewall policies that match list of IP addresses and netmasks you specify. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25". Multiple address/netmask pairs should be separated with commas.

### Examples

The following example displays information about all firewall policies:

```
cluster1::> system services firewall policy show
4 entries were displayed.
```

Policy	Service	Action	IP-List
cluster	dns	allow	0.0.0.0/0
	http	allow	0.0.0.0/0
	https	allow	0.0.0.0/0
	ntp	allow	0.0.0.0/0
	rsh	allow	0.0.0.0/0
	snmp	allow	0.0.0.0/0
	ssh	allow	0.0.0.0/0
	telnet	allow	0.0.0.0/0
data	dns	allow	0.0.0.0/0
	http	deny	0.0.0.0/0
	https	deny	0.0.0.0/0
	ntp	deny	0.0.0.0/0
	rsh	deny	0.0.0.0/0
	snmp	deny	0.0.0.0/0
	ssh	deny	0.0.0.0/0
	telnet	deny	0.0.0.0/0
intercluster	dns	deny	0.0.0.0/0
	http	deny	0.0.0.0/0
	https	deny	0.0.0.0/0
	ntp	deny	0.0.0.0/0
	rsh	deny	0.0.0.0/0
	snmp	deny	0.0.0.0/0
	ssh	deny	0.0.0.0/0
	telnet	deny	0.0.0.0/0
mgmt	dns	allow	0.0.0.0/0
	http	allow	0.0.0.0/0
	https	allow	0.0.0.0/0
	ntp	allow	0.0.0.0/0
	rsh	deny	0.0.0.0/0
	snmp	allow	0.0.0.0/0
	ssh	allow	0.0.0.0/0
	telnet	allow	0.0.0.0/0

32 entries were displayed.

---

## system services manager install show

Display a list of installed services

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services manager install show` command displays information about installed services.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use '`-fields ?`' to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**service** <text>] - Service

Use this parameter to display information only about installed services that have the name you specify.

[-**version** <service version>] - Version

Use this parameter to display information only about installed services that have the version number you specify.

[-**constituent** <text>] - Constituent

Use this parameter to display information only about installed services that have the constituent process you specify.

[-**nodes** {<nodename>|local}, ...] - Nodes

Use this parameter to display information only about services that are installed on the nodes you specify.

[-**description** <text>] - Description



---

Use this parameter to display information only about installed services that match the description you specify.

**Examples**

The following example shows typical output from a two-node cluster.

```
cluster1::> system services manager install show
Service          Version Constituent Nodes
-----
antivirus         1.0      avs      node1, node2
diagnosis         1.0      schmd    node1, node2
                  1.0      shmd     node1, node2
3 entries were displayed.
```

---

## system services manager policy add

Add a new service policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services manager policy add` command adds a new service policy to the services manager. Policies determine which versions of a service can run on the nodes of the cluster.

### Parameters

**-service** <text> - Service

Use this parameter to specify the name of the service for which to add a policy.

**-version** <service version> - Version

Use this parameter to specify the minimum version number of the service to run.

### Examples

This example adds a service manager policy for version 1.0 of the antivirus service.

```
cluster1::> system services manager policy add -service antivirus -version 1.0
```

## system services manager policy remove

Remove a service policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services manager policy remove` command removes a policy from the services manager. Policies determine which versions of a service can run on the nodes of the cluster.

### Parameters

---

**-service** <text> - Service

Use this parameter to specify the name of the service from which to remove a policy.

**-version** <service version> - Version

Use this parameter to specify the version number that is configured by the policy to remove.

## Examples

The following example shows the removal of the service policy for version 1.0 of the antivirus service.

```
cluster1::>system services manager policy remove -service antivirus -version 1.0
```

## system services manager policy setstate

Enable/disable a service policy

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system services manager policy setstate` command enables or disables services manager policies. Use the `system services manager policy show` command to display information about configured policies.

## Parameters

**-service** <text> - Service

Use this parameter to set the state of the policy you specify.

**-version** <service version> - Version

Use this parameter to set the state of the policy with the version number you specify.

**-state** {on|off} - State

Use this parameter with the value "on" to enable the policy. Use this parameter with the value "off" to disable the policy.

## Examples

The following example sets the policy for version 1.0 of the antivirus service to off.

---

```
cluster1::> system services manager policy setstate -service antivirus -version  
1.0 -state off
```

## See Also

`system services manager policy show`

---

## system services manager policy show

Display service policies

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services manager policy show` command displays information about policies that determine which versions of a service can run on the nodes of the cluster.

Use the `system services manager status show` command to view information about services that are configured to run in the cluster.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**service** <text>] - Service

Selects policies that apply to the service you specify.

[-**version** <service version>] - Version

Selects policies that have the version number you specify.

[-**constituent** <text>] - Constituent

Selects policies that have the constituent process you specify.

[-**state** {on|off}] - State

Use this parameter with the value "on" to select information about policies that are currently active. Use this parameter with the value "off" to select information about policies that are not currently active.

[-**num-active** <integer>] - Number Active

---

Selects policies that have the number of active (running) instances you specify.

**[-target-nodes <service affinity>, ...]** - Target Nodes

Selects policies that are configured to run on the nodes you specify.

**[-tag <UUID>]** - Tag (privilege: advanced)

Selects policies that have the UUID you specify. Use this parameter with the `-fields` parameter to display a list of the UUIDs of configured services.

### Examples

The following example shows typical output for this command.

```
cluster1::> system services manager policy show
Service          Version State Constituent Number Target
                  Active Nodes
-----
antivirus         1.0    off   avs          0      any
diagnosis         1.0    on    schmd         1      any
                  1.0    on    shmd         1      any
3 entries were displayed.
```

### See Also

`system services manager status show`

---

## system services manager status show

Display the status of a service

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services manager status show` command displays the status of system services that are configured to run in the cluster.

System services run on the nodes of the cluster based on policies. Policies determine which versions of a service can run on the nodes of the cluster. Use the `system services manager policy show` command to view existing policies.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**service** <text>] - Service

Selects information about services that match the service name you specify.

[-**version** <service version>] - Version

Selects information about services that are configured to run the version number you specify. The configured version is the minimum version that is allowed to run in the cluster according to a policy. Use the `system services manager policy show` command to view information about service policies.

[-**constituent** <text>] - Constituent

Selects information about services that have the constituent process you specify.

[-**actual-version** <service version>] - Actual Version

Selects information about services that are running the version number you specify. This number can be higher than the configured version if a more recent version is installed on the node that is running the service.

**[-node <nodename>]** - Node

Selects information about services that the services manager has assigned to run on the nodes you specify. If the service state is "running", the service is running on these nodes.

**[-state <svc\_state>]** - State

Selects information about services that are in the state you specify.

**[-is-running {true|false}]** - Is Running

Use this parameter with the value "true" to select information about services that are currently running. Use this parameter with the value "false" to select information about services that are not currently running.

Examples

The example below shows typical output for a simple cluster.

```
cluster1::>system services manager status show
Service          Version Constituent Actual Version Node State
-----
diagnosis          1.0      schmd      1.0      cluster1-01 running
                   1.0      shmd       1.0      cluster1-01 running
2 entries were displayed.
```

See Also

system services manager policy show



---

## system services ndmp kill-all

Kill all NDMP sessions

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp kill-all` command is used to terminate all NDMP sessions on a particular node in the cluster. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

Node on which all NDMP sessions needs to be terminated.

### Examples

The following example shows how all NDMP sessions on the node named node1 can be terminated:

```
cluster1::> system services ndmp kill-all -node node1
```

## system services ndmp kill

Kill the specified NDMP session

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp kill` command is used to terminate a specific NDMP session on a particular node in the cluster. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

---

Name of the node on which NDMP session needs to be terminated.

<integer> - Session Identifier

Session ID of the NDMP session.

## Examples

The following example shows how a specific NDMP session on the node named node1 can be terminated:

```
cluster1::> system services ndmp kill 4323 -node node1
```

## See Also

system services ndmp killsession

---

## system services ndmp modify

Modify NDMP service configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp modify` command allows you to modify the NDMP configurations for a node in the cluster. One or more of the following configurations can be modified:

- Enable/disable NDMP service
- Enable/disable sending the NDMP password in clear text. Note that MD5 authentication mode is always enabled.
- NDMP user ID

This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node whose NDMP configuration is to be modified.

**[-enable** {true|false}] - NDMP Service Enabled

This optionally specifies whether NDMP is enabled on the node. The default setting is `true`.

**[-clear-text** {true|false}] - Allow Clear Text Password

This optionally specifies whether the NDMP password can be sent in clear text. The default setting is `true`.

**[-user-id** <text>] - NDMP User ID

This optionally specifies the ID of the NDMP user.

**[-common-sessions** <integer>] - NDMP Common Sessions (privilege: advanced)

This optional parameter specifies the number of extra common NDMP sessions supported, in addition to the number of backup and restore sessions supported for a platform. The default value is 4 for all platforms. The number of backup and restore sessions are platform dependent.

---

Warning: Increasing this parameter can make the storage system unresponsive.

## Examples

The following example modifies the NDMP configuration on a node named node1. The configuration enables NDMP, disables sending the password in clear text, and specifies an NDMP user named ndmp:

```
cluster1::> system services ndmp modify -node node1 -enable true
               -clear-text false -user-id ndmp
```

## system services ndmp off

Disable NDMP service

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system services ndmp off` command is used to disable the NDMP service on any node in the cluster. This command is not supported on Infinite Volumes.

## Parameters

**-node** {<nodename>|local} - Node

The specific node on which NDMP service is to be disabled.

**[-enable** {true|false}] - NDMP Service Enabled

This optionally specifies whether NDMP is enabled on the node. The default setting is `true`.

**[-clear-text** {true|false}] - Allow Clear Text Password

This optionally specifies whether the NDMP password can be sent in clear text.

**[-user-id** <text>] - NDMP User ID

This optionally specifies the ID of the NDMP user.

**[-common-sessions** <integer>] - NDMP Common Sessions (privilege: advanced)

(Description not available)

## Examples

---

The following example is used to turn off the NDMP service on node named node1:

```
cluster1::> system services ndmp off -node node1
```

## **See Also**

`system services ndmp modify`

---

## system services ndmp on

Enable NDMP service

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp on` command is used to enable the NDMP service across any node in the cluster. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

The specific node on which the NDMP service is to be enabled.

**[-enable** {true|false}] - NDMP Service Enabled

This optionally specifies whether NDMP is enabled on the node. The default setting is `true`.

**[-clear-text** {true|false}] - Allow Clear Text Password

This optionally specifies whether the NDMP password can be sent in clear text.

**[-user-id** <text>] - NDMP User ID

This optionally specifies the ID of the NDMP user.

**[-common-sessions** <integer>] - NDMP Common Sessions (privilege: advanced)

(Description not available)

### Examples

The following example is used to turn on the NDMP service on node named node1:

```
cluster1::> system services ndmp on -node node1
```

### See Also

`system services ndmp modify`

---

## system services ndmp password

Change the NDMP password for the node

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp password` command is used to change the NDMP password for a node in the cluster. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

The specific node for which the password is to be changed.

### Examples

The following example is used to change the NDMP password for the node named `node1`:

```
cluster1::> system services ndmp password -node node1
Please enter password:
Confirm password:
```

## system services ndmp probe

Display list of NDMP sessions

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp probe` command displays diagnostic information about all the NDMP sessions in the cluster. The following fields are displayed for each of the sessions:

- Node
- Session identifier

- 
- NDMP version
  - Session authorized
  - Data state
  - Data operation
  - Data server halt reason
  - Data server connect type
  - Data server connect address
  - Data server connect port
  - Data bytes processed
  - Mover state
  - Mover mode
  - Mover pause reason
  - Mover halt reason
  - Mover record size
  - Mover record number
  - Mover bytes moved
  - Mover seek position
  - Mover bytes left to read
  - Mover window offset
  - Mover window length
  - Mover position
  - Mover SetRecordSize flag
  - Mover SetWindow flag
  - Mover connect type
  - Mover connect address
  - Mover connect port
  - Effective host
  - NDMP client address



- 
- NDMP client port
  - SCSI device ID
  - SCSI hostadapter
  - SCSI target ID
  - SCSI LUN ID
  - Tape device
  - Tape mode

This command is not supported on Infinite Volumes.

## Parameters

**-node** {<nodename>|local} - Node

If this parameter is specified, the command displays information about the sessions running on the specified node only. Node should be a valid node name.

**-session-id** <integer> - Session Identifier

If this parameter is specified, the command displays information only about the specified session.

## Examples

The following example displays diagnostic information about all the sessions in the cluster:

```
cluster1::> system services ndmp probe
      Node: clus1-01
      Session identifier: 4952
      NDMP version: 4
      Session authorized: true
      Data state: IDLE
      Data operation: NOACTION
      Data server halt reason: NA
      Data server connect type: LOCAL
      ....
      ....
      Node: clus1-02
      Session identifier: 5289
      NDMP version: 4
      Session authorized: true
      Data state: IDLE
      Data operation: NOACTION
      Data server halt reason: NA
      Data server connect type: LOCAL
      ....
      ....
```

---

The following example displays diagnostic information of sessions running on the node `clus1-01` only:

```
cluster1::> system services ndmp probe -node clus1-01
      Node: clus1-01
    Session identifier: 4952
      NDMP version: 4
    Session authorized: true
      Data state: IDLE
    Data operation: NOACTION
  Data server halt reason: NA
Data server connect type: LOCAL
  ...
```

## See Also

`system services ndmp status`

---

## system services ndmp show

Display NDMP service configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp show` command displays the following information about the NDMP configuration across all the nodes in the cluster:

- Node name
- Whether NDMP is enabled on the node
- Whether sending the NDMP password in clear text is enabled on the node
- NDMP user ID

A combination of parameters can be optionally supplied to filter the results based on specific criteria. This command is not supported on Infinite Volumes.

### Parameters

{ [-**fields** <fieldname>, ...]

If this parameter is specified, the command displays only the fields that you specify.

| [-**instance** ] }

If this parameter is specified, the command displays detailed information about all entries.

[-**node** {<nodename>|local}] - Node

Selects information about the specified node.

[-**enable** {true|false}] - NDMP Service Enabled

Selects information about the nodes where NDMP is enabled/disabled.

[-**clear-text** {true|false}] - Allow Clear Text Password

Selects information about the nodes whose clear-text setting matches the specified value.

[-**user-id** <text>] - NDMP User ID

---

Selects information about the nodes that have the specified NDMP user ID.

**[-common-sessions <integer>]** - NDMP Common Sessions (privilege: advanced)

Selects information about the nodes that have the specified number of NDMP common sessions.

### Examples

The following example displays information about the NDMP configuration of all nodes in the cluster:

```
cluster1::> system services ndmp show
Node      Enabled  Clear text  User Id
-----
node0     true     true       ndmp
node1     true     true       ndmp
node2     true     true       ndmp
node3     true     true       ndmp
4 entries were displayed.
```

---

## system services ndmp start

Start the NDMP service

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system services ndmp start` command starts the NDMP service daemon for a node. This is different from the `system services ndmp on` command. The `system services ndmp on` command enables the daemon to accept NDMP requests. The NDMP service daemon starts automatically on a node when it boots up. Use this command to start the NDMP service daemon that has been stopped by the `system services ndmp stop` command. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the NDMP service needs to be started.

### Examples

```
cluster1::*> system services ndmp start -node node0
```

Starts the NDMP service on node0.

### See Also

`system services ndmp on`   `system services ndmp stop`

---

## system services ndmp status

Display list of NDMP sessions

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ndmp status` command lists all the NDMP sessions in the cluster. By default it lists the following details about the active sessions:

- Node
- Session ID

A combination of parameters can be optionally supplied so as to list only those sessions which match specific conditions. A short description of each of the parameter is provided in the parameters section. This command is not supported on Infinite Volumes.

### Parameters

{ **[-fields** <fieldname>, ...]

This optional parameter specifies which all additional fields to display. Any combination of the following fields are valid:

- ndmp-version
- session-authorized
- data-state
- data-operation
- data-halt-reason
- data-con-addr-type
- data-con-addr
- data-con-port
- data-bytes-processed
- mover-state
- mover-mode

- 
- mover-pause-reason
  - mover-halt-reason
  - mover-record-size
  - mover-record-num
  - mover-bytes-moved
  - mover-seek-position
  - mover-bytes-left-to-read
  - mover-window-offset
  - mover-window-length
  - mover-position
  - mover-setrecordsize-flag
  - mover-setwindow-flag
  - mover-con-addr-type
  - mover-con-addr
  - mover-con-port
  - eff-host
  - client-addr
  - client-port
  - spt-device-id
  - spt-ha
  - spt-scsi-id
  - spt-scsi-lun
  - tape-device
  - tape-modes

| [-instance ] }

If this parameter is specified, the command displays detailed information about all the active sessions.

[-node {<nodename>|local}] - Node

---

If this parameter is specified, the command displays information about the sessions running on the specified node only. Node should be a valid node name.

**[-session-id <integer>]** - Session Identifier

If this parameter is specified, the command displays information about specific NDMP session. A session-id is a number used to identify a particular NDMP session.

**[-ndmp-version <integer>]** - NDMP Version

This parameter refers to the NDMP protocol version being used in the session.

**[-session-authorized {true|false}]** - Session Authorized

This field indicates whether an NDMP session is authenticated or not.

**[-data-state <component state>]** - Data State

This field identifies the current state of the data server's state machine.

**[-data-operation <data operation>]** - Data Operation

This field identifies the data server's current operation.

**[-data-halt-reason <halt reason>]** - Data Server Halt Reason

This field identifies the event that caused the data server state machine to enter the HALTED state.

**[-data-con-addr-type <address type>]** - Data Server Connect Type

This field specifies the type of data connection established by the data server. The data connection can be established locally within a given system or between remote networked systems.

**[-data-con-addr <text>]** - Data Server Connect Address

This specifies the connection endpoint information for the data server's data connection.

**[-data-con-port <integer>]** - Data Server Connect Port

This specifies the TCP/IP port that the data server will use when establishing a data connection.

**[-data-bytes-processed <integer>]** - Data Bytes Processed

This field represents the cumulative number of data stream bytes transferred between the backup or recovery method and the data connection during the current data operation.

**[-mover-state <component state>]** - Mover State



---

This parameter identifies the current state of the NDMP tape server's mover state machine.

**[-mover-mode <mover mode>]** - Mover Mode

This parameter identifies the direction of the mover data transfer.

**[-mover-pause-reason <pause reason>]** - Mover Pause Reason

This parameter identifies the event that caused the mover state machine to enter the PAUSED state.

**[-mover-halt-reason <halt reason>]** - Mover Halt Reason

This integer field identifies the event that caused the mover state machine to enter the HALTED state.

**[-mover-record-size <integer>]** - Mover Record Size

This field represents the current mover record size in bytes.

**[-mover-record-num <integer>]** - Mover Record Number

This field represents the last tape record processed by the mover.

**[-mover-bytes-moved <integer>]** - Mover Bytes Moved

This field represents the cumulative number of data stream bytes written to the data connection or the number of data stream bytes read from the data connection and written to the tape subsystem, depending on the mode of mover operation.

**[-mover-seek-position <integer>]** - Mover Seek Position

This field represents the data stream offset of the first byte the DMA requested the mover to transfer to the data connection during a mover read operation.

**[-mover-bytes-left-to-read <integer>]** - Mover Bytes Left to Read

This field represents the number of data bytes remaining to be transferred to the data connection to satisfy the current NDMP\_MOVER\_READ request.

**[-mover-window-offset <integer>]** - Mover Window Offset

This field represents the absolute offset of the first byte of the mover window within the overall data stream.

**[-mover-window-length <integer>]** - Mover Window Length

This field represents the length of the current mover window in bytes.

**[-mover-position <integer>]** - Mover Position

---

This parameter can be used to list only those sessions, whose mover position matches a specific value. Mover-position should be an integer.

**[-mover-setrecordsize-flag {true|false}]** - Mover SetRecordSize Flag

This field is used by the DMA to establish the record size used for mover-initiated tape read and write operations.

**[-mover-setwindow-flag {true|false}]** - Mover SetWindow Flag

This flag represents whether a mover window has been set or not. A mover window represents the portion of the overall backup stream that is accessible to the mover without intervening DMA tape manipulation.

**[-mover-con-addr-type <address type>]** - Mover Connect Type

This field specifies the type of data connection established by the mover. The data connection can be established locally within a given system or between remote networked systems.

**[-mover-con-addr <text>]** - Mover Connect Address

This specifies the endpoint address or addresses that the mover will use when establishing a data connection.

**[-mover-con-port <integer>]** - Mover Connect Port

This specifies the TCP/IP port that the mover will use when establishing a data connection.

**[-eff-host <host type>]** - Effective Host

This field indicates the host context in which the NDMP session runs. The valid values are: PRIMARY or PARTNER.

**[-client-addr <text>]** - NDMP Client Address

This parameter specifies the client's IP address.

**[-client-port <integer>]** - NDMP Client Port

This parameter specifies the client's port number.

**[-spt-device-id <text>]** - SCSI Device ID

This parameter specifies the SCSI device ID.

**[-spt-ha <integer>]** - SCSI Host Adapter

This parameter specifies the SCSI host adapter.

**[-spt-scsi-id <integer>]** - SCSI Target ID

---

This parameter specifies the SCSI target.

**[-spt-scsi-lun <integer>]** - SCSI LUN ID

This parameter specifies the SCSI LUN ID.

**[-tape-device <text>]** - Tape Device

This parameter specifies the name to identify the tape device.

**[-tape-mode <mover mode>]** - Tape Mode

This parameter specifies the mode in which tapes are opened.

## Examples

The following example displays all the NDMP sessions on the cluster:

```
cluster1::> system services ndmp status
                Session
Node
-----
node-01        17479
node-01        19769
node-02        21118
3 entries were displayed.
```

The following example shows how to display only the sessions running on node-01:

```
cluster1::> system services ndmp status -node node-01
                Session
Node
-----
node-01        17479
node-01        19769
2 entries were displayed.
```

## system services ndmp stop

Stop the NDMP service

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system services ndmp stop` command stops the NDMP service daemon on a node. This is a disruptive command and should not be used in normal scenarios. Processing of active sessions continues but the ability to view or kill sessions is lost. This is different from the `system services ndmp off` command. The `system services ndmp off` command disables new NDMP connections on the node but

---

does not stop the NDMP service daemon. This command is not supported on Infinite Volumes.

## Parameters

**-node** {<nodename>|local} - Node

The node on which the NDMP service needs to be stopped.

## Examples

```
cluster1::*> system services ndmp stop -node node0
```

Stops the NDMP service on node0.

## See Also

system services ndmp off   system services ndmp start

---

## system services ndmp terminate

Terminate all NDMP sessions

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `system services ndmp terminate` command terminates all active sessions on the node. This command forcefully terminates all NDMP sessions without an opportunity for a graceful shutdown. Use `system services ndmp kill-all` for a clean termination of all active sessions on a node. This command is not supported on Infinite Volumes.

### Parameters

**-node** {<nodename>|local} - Node

The node on which the NDMP sessions need to be terminated

### Examples

```
cluster1::*> system services ndmp terminate -node node0
```

Terminates all active NDMP sessions on node0.

### See Also

`system services ndmp kill-all`

---

## system services ndmp log start

Start logging for the specified NDMP session

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

This command is used to start logging on an active NDMP session on a node. You can start logging two different kinds of sessions. The NDMP server session manages all NDMP tasks on the node. If you want to log information regarding the NDMP server, use `server` with the `-session-id` parameter to enable logging. If you want to log information about a particular NDMP session, for example a restore operation, then determine the session ID for the session using the "system services ndmp status" command and use that ID with the `-session-id` parameter to enable logging.

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node.

**-session-id** {<integer>|server} - Session Identifier

This parameter specifies the NDMP session-id on which logging needs to be started. The session-id is associated with a unique NDMP session. Specify `server` to start logging on the NDMP server session.

**-filter** <text> - Level Filter

Use this parameter to specify the filter for a particular session ID. This parameter controls the NDMP modules for which logging is to be enabled. This parameter can take five values. They are as follow : `all`, `none`, `normal`, `backend` or "filter-expression". The default value for this is `none`.

- `all` turns on logging for all modules.
- `none` disables logging for all modules.
- `normal` is a short cut parameter that enables logging for all modules except `verbose` and `io_loop`. The equivalent filter string is `all-verbose-io_loop`
- `backend` is a short cut parameter that enables logging for all modules except `verbose`, `io_loop`, `ndmps` and `ndmpd`. The equivalent filter string is `all-verbose-io_loop-ndmps-ndmpp`

- (filter-expression) is a combination of one or more modules for which logs needs to be enabled. Multiple module names can be combined using following operators :
  - - to remove the given module from the list of specified modules in the filter string. For example the filter all-ndmpps will enable logging for all modules but not ndmpps.
  - ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter ndmpps^mover^data will enable logging for ndmpps, mover and data.

The possible module names and a brief description is given below:

		Modules	Description
		verbose	verbose message
		io	I/O process loop
messages		io_loop	I/O process loop verbose
		ndmps	NDMP service
		ndmpp	NDMP Protocol
		rpc	General RPC service
		fdc_rpc	RPC to FC driver service
		auth	Authentication
		mover	NDMP MOVER (tape I/O)
restore)		data	NDMP DATA (backup/
ops)		scsi	NDMP SCSI (robot/tape
client		bkup_rpc	RPC to Backup service
server		bkup_rpc_s	RPC to Backup service
cleaner		cleaner	Backup/Mover session
reconfigure		conf	Debug configure/
		dblade	Dblade specific messages
messages		timer	NDMP server timeout
		vldb	VLDB service
		smf	SMF Gateway messages
		vol	VOL OPS service
		sv	SnapVault NDMP extension
		common	NDMP common state
		ext	NDMP extensions messages
		sm	SnapMirror NDMP extension

## Examples

The following example shows how to start logging on a specific NDMP session 33522, running on the node cluster1-01 with filter normal.

```
cluster1::*> system services ndmp log start -node
cluster1-01 -session-id 33522 -filter normal
```

The following example shows how to start logging on the NDMP server session, on the node cluster1-01 with filter all.

```
cluster1::*> system services ndmp log start -session-id
server -filter all -node cluster1-01
```

## system services ndmp log stop

Stop logging for the specified NDMP session

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

## Description

This command is used to stop logging on an active NDMP session on a node. The NDMP server session manages all NDMP tasks on the node. If you want to stop logging information regarding the NDMP server, use `server` with the `-session-id` parameter to disable logging. If you want to stop logging information about a particular NDMP session, for example a restore operation, then determine the session ID for the session using the "system services ndmp status" command and use that ID with the `-session-id` parameter to disable logging.

## Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node.

**-session-id** {<integer>|server} - Session Identifier

This parameter specifies the NDMP session-id on which logging needs to be stopped. The session-id is associated with a unique NDMP session. Specify `server` to stop logging on the NDMP server session.



---

## Examples

The following example shows how to stop logging on a specific NDMP session 35512, running on node cluster1-01.

```
cluster1::*>system services ndmp log stop -session-id  
35512 -node cluster1-01
```

The following example shows how to stop logging on the NDMP server session, running on node cluster1-01.

```
cluster1::*>system services ndmp log stop -session-id server -  
node cluster1-01
```

## system services ndmp node-scope-mode off

Disable NDMP node-scope-mode

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command puts NDMP server in Vserver-aware mode. The Vserver-aware commands are available under `vserver services ndmp`.

### Parameters

None

## Examples

The following example shows how to disable the node-scope-mode of NDMP server.

```
cluster1::> system services ndmp node-scope-mode off  
NDMP node-scope-mode is disabled.
```

## See Also

`vserver services ndmp`

---

## system services ndmp node-scope-mode on

Enable NDMP node-scope-mode

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command puts the NDMP server in the node-scope-mode. In the node-scope-mode, NDMP server has the following behavior:

- All NDMP operations are restricted to resources on the node
- Vserver-aware NDMP commands are disabled
- NDMP authentication falls back to DATA ONTAP 8.1 NDMP authentication scheme

### Parameters

None

### Examples

The following example enables node-scope-mode of operation :

```
cluster1::> system services ndmp node-scope-mode on
NDMP node-scope-mode is enabled.
```

## system services ndmp node-scope-mode status

Status of NDMP node-scope-mode

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays whether the NDMP server is operating in node-scope-mode or not.

- NDMP node-scope-mode is disabled - NDMP server is Vserver-aware

- 
- NDMP node-scope-mode is enabled - NDMP server is node scoped

## Parameters

None

## Examples

The following example shows how to check the status of NDMP server in a cluster

```
cluster1::> system_services ndmp node-scope-mode status
NDMP node-scope-mode is disabled.
```

## system services ntp server create

Add a NTP Server

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system services ntp server create` command associates a node with an NTP server.

## Parameters

**-node** {<nodename>|local} - Node

This specifies the node with which the NTP server is to be associated.

**-server** <text> - NTP Server Name or IP Address

This specifies the name or IP address of the NTP server that is to be associated with the specified node.

**[-preferred** {true|false}] - Preferred NTP Server (privilege: advanced)

This optionally specifies whether the specified NTP server is the preferred NTP server for the node to use. The default setting is `false`. This parameter is available only at the advanced privilege level and higher.

**[-version** {1|2|3|4|max}] - NTP Version for Server

---

This optionally specifies the version of NTP that is running on the specified NTP server. Possible values include 1, 2, 3, 4, and max (for the highest-numbered version currently available). The default setting is `max`.

## Examples

The following example associates a node named `node2` with an NTP server named `ntp1.example.com` that is running the highest-numbered version of NTP available.

```
cluster1::> system services ntp server create -node node2 -server
ntp1.example.com -version max
```

## system services ntp server delete

Delete a NTP Server

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system services ntp server delete` command deletes an NTP server from a specified node's NTP configuration.

## Parameters

**-node** {<nodename>|local} - Node

This specifies the node from which the NTP server is to be deleted.

**-server** <text> - NTP Server Name or IP Address

This specifies the name or IP address of the NTP server that is to be removed from the node's NTP configuration.

## Examples

The following example deletes an NTP server named `ntp2.example.com` from the NTP configuration of a node named `node3`:

```
cluster1::> system services ntp server delete -node node3 -server
ntp2.example.com
```

## system services ntp server modify

---

## Modify NTP Server Options

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system services ntp server modify` command modifies whether an NTP server is the preferred server for a node, the NTP version associated with an NTP server, or both.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the node on which the NTP server is to be modified.

**-server** <text> - NTP Server Name or IP Address

This specifies the name or IP address of the NTP server whose version is to be modified.

**[-preferred** {true|false}] - Preferred NTP Server (privilege: advanced)

This optionally specifies whether the specified NTP server is the preferred NTP server for the node to use. The default setting is `false`. This parameter is available only at the advanced privilege level and higher.

**[-version** {1|2|3|4|max}] - NTP Version for Server

This optionally specifies the version of NTP that is running on the specified NTP server. Possible values include 1, 2, 3, 4, and max (for the highest-numbered version currently available). The default setting is `max`.

### Examples

The following example modifies the NTP version associated with an NTP server named `ntp2.example.com` used by a node named `node3`. The NTP version is changed to 4.

```
cluster1:> system services ntp server modify -node node3 -server  
ntp2.example.com -version 4
```

## system services ntp server show

Display a list of NTP Servers

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

---

## Description

The `system services ntp server show` command displays the following information about NTP servers associated with nodes in a cluster:

- Node name
- NTP server name or IP address
- NTP version running on the NTP server
- Whether the NTP server is the preferred NTP server for the node (advanced privilege level or higher only)

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**node** {<nodename>|local}] - Node

If this parameter is specified by itself, the command displays information only about the specified node; if the parameter is specified with the `-server` parameter, the command displays detailed information about the association between the specified node and NTP server.

[-**server** <text>] - NTP Server Name or IP Address

If this parameter is specified by itself, the command displays information only about the node or nodes that use the specified NTP server; if the parameter is specified with the `-node` parameter, the command displays detailed information about the association between the specified node and NTP server. The value for this parameter can be either a name or IP address.

[-**preferred** {true|false}] - Preferred NTP Server (privilege: advanced)

If this parameter is specified, the command displays information only about any node or nodes that have a preferred NTP server. This parameter is available only at the advanced privilege level and higher.

[-**version** {1|2|3|4|max}] - NTP Version for Server

---

If this parameter is specified, the command displays information only about the node or nodes associated with an NTP server or servers that are running the specified version of NTP.

**Examples**

The following example displays information about all associations between nodes and NTP servers:

```
cluster1::> system services ntp show
Node  Server  Version
-----
node0  ntp1.example.com  max
      ntp2.example.com  max
node1  ntp1.example.com  max
      ntp2.example.com  max
node2  ntp1.example.com  max
      ntp2.example.com  max
node3  ntp1.example.com  max
      ntp2.example.com  max
```

---

## system services web modify

Modify the cluster-level configuration of web protocols

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command modifies the overall availability of web services in the cluster, including the core protocol configurations for those services. In a pre-root or unclustered scenario, its scope applies to the local node.

Note:

You cannot disable Transport Layer Security (TLS).

### Parameters

**[-external {true|false}]** - External Web Services

Defines whether remote clients can access HTTP or HTTPs service content. Along with the `system services firewall` configuration, this parameter controls the visibility for client connections. The default value for this parameter after installation is 'true', which exports web protocols for remote access. If no value is provided during modification, its behavior does not change.

**[-sslv3-enabled {true|false}]** - SSLv3 Enabled

Defines whether the SSL-enabled Vservers in the cluster support Secure Socket Layer version 3. The default value for this parameter after installation is 'true', which enables SSLv3.

**[-sslv2-enabled {true|false}]** - SSLv2 Enabled

Defines whether SSL-enabled Vservers in the cluster support Secure Socket Layer version 2. The default value for this parameter after installation is 'false', which disables SSLv2.

### Examples

The following command enables SSL version 2 support:

```
cluster1::*> system services web modify -sslv2-enabled true
```

Warning: Modifying the cluster configuration will cause pending web service requests to be interrupted as the web servers are restarted.



---

Do you want to continue? {y|n}: y

## See Also

system services firewall

---

## system services web show

Display the cluster-level configuration of web protocols

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the overall availability of web services in the cluster, including the core protocol configurations for those services. In a pre-root or unclustered scenario, its output applies to the local node. The following information explains the `external` and `status` attributes, two features of web services' availability.

The `external` parameter defines whether remote clients are allowed to access the HTTP or HTTPs service content. Along with the `system services firewall` configuration, the `external` parameter controls the visibility for client connections.

The `status` parameter describes the aggregated operational state of cluster-level web services as retrieved from the `system services web node` command. The `status` parameter does not reflect whether the protocols are externally visible, but whether the server processes are running correctly. For detailed information about individual servers, use the `system services web node show` command. The following are the possible values for the `status` in node configuration or availability:

- `online`, indicates that all web services are consistently configured and working correctly.
- `partial`, indicates that one or more nodes' web services are unavailable due to an error condition.
- `mixed`, indicates that the nodes in the cluster do not share the same web services configuration. This situation might occur if individual nodes were reconfigured with the `system services web node` command.
- `offline`, indicates that all of the nodes' web services are unavailable due to an error condition.
- `unclustered`, indicates that the current node is not part of an active cluster.

### Parameters

None

---

## Examples

The following example displays the availability of web services for the cluster.

```
clus01::system services web> show
External Web Services: true
                        Status: online
  HTTP Protocol Port: 80
  HTTPS Protocol Port: 443
    TLSv1 Enabled: true
    SSLv3 Enabled: true
    SSLv2 Enabled: false
```

## See Also

system services firewall   system services web node   system services web node show

---

## system services web node show

Display the status of the web servers at the node level

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays operational configuration for the web server processes on the nodes in the cluster. This output is aggregated to produce the content for the `system services web show` command.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

Identifies the node where the web server process is being executed.

[-external {true|false}] - External Web Services

Defines whether remote clients can access the HTTP or HTTPs service content. Along with the `system services firewall` configuration, this parameter controls the visibility for client connections. The default value for this parameter after installation is 'true', which exports web protocols for remote access.

[-http-port <integer>] - HTTP Port

Defines the HTTP port for the node-level web services.

[-https-port <integer>] - HTTPs Port

Defines the encrypted HTTP (HTTPs) port for the node-level web services.

[-tlsv1-enabled {true|false}] - TLSv1 Enabled

---

Defines whether the SSL-enabled services supplied by the node support Transport Layer Security version 1. You cannot set the value of this parameter to 'false' when using the `system services web node modify` command.

**[-sslv3-enabled {true|false}]** - SSLv3 Enabled

Defines whether SSL-enabled services supplied by the node support Secure Socket Layer version 3. The default value of this parameter after the node installation is 'true', which enables SSLv3.

**[-sslv2-enabled {true|false}]** - SSLv2 Enabled

Defines whether SSL-enabled services supplied by the node support Secure Socket Layer version 2. The default value for this parameter after the node installation is 'false', which disables SSLv2.

**[-status {offline|partial|mixed|online|unclustered}]** - Protocol Status

Describes the operational state of node-level web services. This parameter does not reflect whether protocols are externally visible, but whether the server processes are running correctly. The following are the possible values that describe the service availability.

- `online`, indicates that web services are working correctly.
- `offline`, indicates that web services are unavailable due to an error condition.
- `unclustered`, indicates that the current node is not part of an active cluster.

**[-total-hits <integer>]** - Total HTTP Requests

Indicates the total number of requests serviced by the web server.

**[-total-bytes <integer>]** - Total Bytes Served

Indicates the total number of bytes returned by the web server.

## Examples

The following example displays the status of web servers for nodes in the cluster.

```
clus01::system services web node> show
```

Node	External	HTTP Port	HTTPs Port	Status	Total HTTP Requests	Total Bytes Served
n6070-8	true	80	443	online	5	3421
n6070-9	true	80	443	online	5	3421

2 entries were displayed.

## See Also

---

system services firewall   system services web node modify  
system services web show

---

## system smtape abort

Abort an active SMTape session

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command aborts the backup or restore operations based on the session identifier. You can perform SMTape operations using the `system smtape backup` or `system smtape restore` commands. A unique session identifier is assigned for each new SMTape operation. This command aborts sessions that are in active and waiting states.

### Parameters

**-session** <Sequence Number> - Session Identifier

Use this parameter to specify the session identifier for a backup or restore session.

### Examples

Abort the SMTape session with the session identifier 20

```
cluster::> system smtape abort -session 20
Abort posted to session 20.
```

### See Also

`system smtape backup` `system smtape restore`

---

## system smtape backup

Backup a volume to tape devices

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command performs a baseline backup of a specified volume path to a tape device. You can use the command `system hardware tape drive show` to view the list of tape devices in the cluster. You must specify a Snapshot copy name to perform an SMTape backup operation. The Snapshot copy name specified is used as the base Snapshot copy. A new unique session ID is assigned for this SMTape operation and the status of the session can be monitored using the command `system smtape status`. This session ID can be subsequently used to perform other operations such as to find the SMTape status, abort an SMTape operation, and continue an SMTape operation.

The volume and tape device must reside on the same node in the cluster. You must retain the base Snapshot copy created during this backup operation in order to use this Snapshot copy to re-establish a SnapMirror relationship upon a restore.

### Parameters

**-vserver** <vserver name> - Vserver Name

Use this parameter to specify the Vserver name on which the volume is located. You need not specify this parameter if only one cluster Vserver exists.

**-volume** <volume name> - Volume Name

Use this parameter to specify the name of the volume that needs to be backed up to tape.

**-backup-snapshot** <snapshot name> - Snapshot Name

Use this parameter to specify the name of the Snapshot copy while performing an SMTape backup operation.

**-tape** </node\_name/tape\_device> - Tape Name

Use this parameter to specify the name of the tape device which is used for this SMTape operation. The format of the tape device name is `/node_name/tape_device`, where `node_name` is the name of the cluster node owning the tape and `tape_device` is the name of the tape device.



---

**[-tape-block-size <integer>]** - Tape Record Size in KB

Use this parameter to specify the tape record size in KB for backup and restore operations. The tape record size is in multiples of 4KB, ranging from 4KB to 256KB. The default tape record size is 240KB unless it is specified.

## Examples

The following example will start the backup of a volume `datavol` in a Vserver `vserver0` to a tape `rst0a`. Both the volume and tape reside on the same node `clus1-01`. The Snapshot copy to be backed up is `datavol_snapshot` and the tape record size has the value of 256KB.

```
clus1::> system smtape backup -vserver vserver0 -volume datavol
        -backup-snapshot datavol_snapshot -tape /clus1-01/rst0a
        -tape-block-size 256
```

Session 21 created successfully

The following example will start the backup of a volume `datavol` in a Vserver `vserver0` to a tape `rst0a`. The volume `datavol` is in a Vserver `vserver0`. Both the volume and tape reside on the same node `clus1-01`. The Snapshot copy to be backed up is `datavol_snapshot` and the tape record size has the default value of 240KB.

```
clus1::> system smtape backup -vserver vserver0 -volume datavol
        -backup-snapshot datavol_snapshot -tape /clus1-01/nrst01
```

Session 22 created successfully

## See Also

`system hardware tape drive show`   `system smtape status`   `system smtape restore`  
`system smtape status show`   `system smtape continue`   `system smtape abort`  
`system node hardware tape drive show`

---

## system smtape break

Make a restored volume read-write

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command breaks the relationship between the tape backup of a volume and a restored volume, changing the restored volume from read-only to read/write.

### Parameters

**-vserver** <vserver name> - Vserver Name

Use this parameter to specify the Vserver name on which the volume is located. You need not specify this parameter if only one cluster Vserver exists.

**-volume** <volume name> - Volume Name

Use this parameter to specify the name of the read-only volume that needs to be made read/writeable after a restore.

### Examples

Make the read-only volume datavol on Vserver vservers0 writeable after a restore.

```
clus1:> system smtape break -vserver vservers0 -volume datavol
[Job 84] Job succeeded: SnapMirror Break Succeeded
```

### See Also

system smtape backup   system smtape restore  
system node hardware tape drive show

---

## system smtape continue

Continue SMTape session waiting at the end of tape

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command continues the SMTape backup and restore operations using the specified tape device. You can use this command when an SMTape operation has reached the end of current tape and is in the wait state to write to or read from a new tape.

If a tape device is not specified, the original tape device will be used.

User has to make sure that the correct tape media is inserted in the device and positioned appropriately before issuing this command.

### Parameters

**[-tape </node\_name/tape\_device>]** - Tape Name

Use this parameter to specify the name of the tape device which is used for this SMTape operation. The format of the tape device name is */node\_name/tape\_device*, where *node\_name* is the name of the cluster node owning the tape and *tape\_device* is the name of the tape device.

**-session <Sequence Number>** - Session Identifier

Use this parameter to specify the session identifier for the SMTape backup or restore operations.

### Examples

Continues an SMTape session having session ID 20 on tape device rst0a on the node node1 in the cluster.

```
cluster::> system smtape continue -session 20 -tape /node1/rst0a
continue on session 20 succeeded
```

The following example continues session 40 on the same tape device that was being used by the session.

```
cluster::> system smtape continue -session 40
continue on session 40 succeeded
```

---

## system smtape restore

Restore a volume from tape devices

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command performs restore of a backup image created using the command `system smtape backup` in the specified tape device to a destination volume path. A new unique session ID is assigned for this operation; the status of the session can be monitored using the command `system smtape status`. It is required that the volume and tape device reside in the same cluster node. The volume must be of type DP (Data Protection) and should be placed in the restricted mode prior to a restore.

Any existing data on the volume will get overwritten upon a restore. The volume will remain as read-only and of type DP after the restore. You can use the command `system smtape break` to get read/write permissions on the volume. Restore to an Infinite Volume is not supported. Restore can be done to a non-root Cluster-Mode DP volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

Use this parameter to specify the Vserver name on which the volume is located. You need not specify this parameter if only one cluster Vserver exists.

**-volume** <volume name> - Volume Name

Use this parameter to specify the volume name on which the tape content will be restored.

**-tape** </node\_name/tape\_device> - Tape Name

Use this parameter to specify the name of the tape device which is used for this SMTape operation. The format of the tape device name is `/node_name/tape_device`, where `node_name` is the name of the cluster node owning the tape and `tape_device` is the name of the tape device.

**[-tape-block-size <integer>]** - Tape Record Size in KB

Use this parameter to specify the tape record size in KB for backup and restore operations. The tape record size is in multiples of 4KB, ranging from 4KB to 256KB. The default tape record size is 240KB unless it is specified. Use the same record size which

---

was used during the backup. If the tape record size is different from the tape record size that was used at the time of backup then `system smtape restore` will fail.

## Examples

The following example will start the restore to a volume `datavol` from a tape `rst0a`. The volume `datavol` is in a Vserver `vserver0`. Both `vserver0` and `rst0a` reside on the same node `clus1-01`.

```
cluster::> system smtape restore -vserver vserver0 -volume datavol
-tape /clus1-01/rst0a -tape-block-size 256

Session 2 created successfully
```

The following example will start the restore to a volume `datavol` from a tape `rst0a`. The volume `datavol` is in a Vserver `vserver0`. Both `vserver0` and `rst0a` reside on the same node `clus1-01`. The default tape record size of 240KB was used during backup.

```
cluster::> system smtape restore -vserver vserver0 -volume datavol
-tape /clus1-01/rst0a

Session 5 created successfully
```

## See Also

`system smtape backup` `system smtape status` `system smtape break`  
`system smtape status show` `system smtape continue`  
`system node hardware tape drive show`

---

## system smtape showheader

Display SMTape header

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the image header of a tape. The tape must have a valid backup of data. The following information about the backup is displayed:

- Tape Number - the tape number if the backup spans multiple tape devices.
- WAFL Version - WAFL version of the storage system when the volume was backed up on tape.
- Backup Set ID - a unique backup set ID for the baseline backup.
- Source Storage System - the source storage system where the volume resided when the backup was performed.
- Source Volume - the source volume that was backed up to tape.
- Source Volume Capacity - the capacity of the source volume that was backed up to tape.
- Source Volume Used Size - the used size of the source volume that was backed up to tape.
- Source Snapshot - name of the Snapshot copy used for the backup.
- Volume Type - type of the volume.
- Is SIS Volume - this field is true if the backed up volume was a SIS volume.
- Backup Version - the SMTape backup version.
- Backup Sequence No - the backup sequence number.
- Backup Mode - this field describes the backup mode.
- Time of Backup - the time at which the backup was performed.
- Time of Previous Backup - the time at which the previous backup was performed; this information is displayed only if the previous backup was an incremental backup.
- Volume Total Inodes - number of inodes of the backed up volume.

- Volume Used Inodes - number of used inodes of the backed up volume.
- Number of Snapshots - number of Snapshot copies present in this backup.
- Snapshot ID - is the Snapshot ID of the backup Snapshot.
- Snapshot Time - time at which the backup Snapshot copy was created.
- Snapshot Name - name of the Snapshot copy which was backed up to tape.

## Parameters

**-tape** </node\_name/tape\_device> - Tape Name

Use this parameter to specify the name of the tape device which is used for this SMTape operation. The format of the tape device name is /node\_name/tape\_device, where node\_name is the name of the cluster node owning the tape and tape\_device is the name of the tape device.

**[-tape-block-size <integer>]** - Tape Record Size in KB

Use this parameter to specify the tape record size in KB for backup and restore operations. The tape record size is in multiples of 4KB, ranging from 4KB to 256KB. The default tape record size is 240KB unless it is specified.

## Examples

The following example reads the image header from the tape nrst01 residing on the node clus1-01 and displays relevant tape header information.

```
clus1::> system smtape showheader -tape /clus1-01/nrst01
-tape-block-size 240

Tape record size in KB: 240
Tape Number: 1
WAFL Version: 23577
Backup Set ID: 7d0c9a15-8e20-11e1-8741-123478563412
Source Storage System: clus1-01
Source Volume: /vsl/srcvol
Source Volume Capacity: 400.00MB
Source Volume Used Size: 0.00
Source Snapshot: mysnap
Volume Type: Flex
Is SISVolume: no
Backup Version: 1:3
Backup Sequence No: 0
Backup Mode: dw-data
Time of Backup: 4/24/2012 15:16:38
Time of Previous Backup: 0/0/0 00:00:00
Volume Total Inodes: 12789
Volume Used Inodes: 100
Number of Snapshots: 1
Snapshot ID: 1
Snapshot Time: 4/24/2012 15:16:10
Snapshot Name: mysnap
```

## See Also

---

system smtape backup   system smtape restore  
system node hardware tape drive show



---

## system smtape status clear

Clear SMTape sessions

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command clears SMTape sessions which are completed, failed or Unknown state.

### Parameters

**[-session <Sequence Number>]** - Session Identifier

Use this parameter to clear the SMTape sessions with the specified session identifier.

**[-node {<nodename>|local}]** - Node Name

Use this parameter to clear the SMTape sessions related to the specified node.

**[-type {backup|restore}]** - Operation Type

Use this parameter to clear the SMTape sessions of the specified operation type. These can be either backup or restore sessions.

**[-status {COMPLETED|FAILED|UNKNOWN}]** - Session Status

Use this parameter to clear the SMTape sessions which have the status as specified in the parameter.

**[-path <text>]** - Path Name

Use this parameter to clear the SMTape sessions which have path as specified in the parameter.

**[-device <text>]** - Device Name

Use this parameter to clear the SMTape sessions on a specific tape device.

**[-backup-snapshot <snapshot name>]** - Snapshot Name

Use this parameter to clear the SMTape sessions using the Snapshot copy name as specified in the parameter.

**[-tape-block-size <integer>]** - Tape Block Size

Use this parameter to clear the SMTape sessions with the tape block size as specified in the parameter.

---

## Examples

The following example clears all the completed SMTape sessions in the cluster:

```
clus1:> system smtape status clear
5 sessions are purged.
```

The SMTape sessions on the node node1 in the cluster are cleared.

```
clus1:> system smtape status clear -node node1
3 sessions are purged.
```

## system smtape status show

Show status of SMTape sessions

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command lists the status of all SMTape sessions in the cluster. By default, this command lists the following entries about each session:

- Session
- Type
- Status
- Progress
- Path
- Device
- Node

### Parameters

{ [-**fields** <fieldname>, ...]

Use this parameter to display additional fields about each session apart from the default entries. This parameter is optional. Any combination of the following fields is valid:

- Session
- Node

- 
- Type
  - Status
  - Path
  - Device
  - Progress
  - Start-time
  - End-time
  - Update-time
  - Backup-snapshot
  - Tape-block-size
  - Error

| **[-instance ]** }

Use this parameter to display detailed information about the specified sessions.

**[-session <Sequence Number>]** - Session Identifier

Use this parameter to display information about a specific SMTape session. A Session Identifier is a number which is used to identify a particular SMTape session.

**[-node {<nodename>|local}]** - Node Name

Use this parameter to display information about sessions related to the specified node.

**[-type {backup|restore}]** - Operation Type

Use this parameter to display information about SMTape sessions of the specified operation type. The operation type could be either a backup or a restore operation.

**[-status {COMPLETED|FAILED|ACTIVE|WAITING|ABORTING|UNKNOWN}]** - Session Status

Use this parameter to display information about SMTape sessions having the specified status in the parameter.

**[-path <text>]** - Path Name

Use this parameter to display information about SMTape sessions on a volume which is at the specified path name. This is the logical path of the volume and you must specify the path name in the following format: /vserver\_name/volume\_name.

**[-device <text>]** - Device Name

---

Use this parameter to display information about the SMTape sessions on the specified tape device. You must specify the tape device name in the following format: `/node_name/tape_device`.

**[-progress {<integer>[KB|MB|GB|TB|PB]}]** - Bytes Transferred

Use this parameter to display information about SMTape sessions in which the number of data bytes transferred in a particular session matches with the number specified in this parameter.

**[-start-time <MM/DD/YYYY HH:MM:SS>]** - Start Time

Use this parameter to display information about SMTape sessions whose starting time matches the specified starting time.

**[-end-time <MM/DD/YYYY HH:MM:SS>]** - End Time

Use this parameter to display information about SMTape sessions whose ending time matches the specified ending time.

**[-backup-snapshot <snapshot name>]** - Snapshot Name

Use this parameter to display information about SMTape sessions that use a particular Snapshot copy name which matches the specified Snapshot copy name in the parameter in backup or restore operations.

**[-tape-block-size <integer>]** - Tape Block Size

Use this parameter to display information about SMTape sessions that use a particular tape block size which matches the specified tape block size parameter in backup or restore operations.

**[-error <text>]** - Error Description

Use this parameter to display information about SMTape sessions that have a particular error description which matches the specified error description in the parameter.

## Examples

Displays default entries about the five SMTape sessions.

```
cluster:::> system smtape status show
```

Session	Type	Status	Progress	Path	Device	Node
5	Backup	COMPLETED	50MB	/vsrvr1/vol1	/cls1-01/nrst01	clus1-01
4	Restore	FAILED	0B	/vsrvr1/vol3	/cls1-02/nrst21	clus1-02
3	Backup	COMPLETED	50MB	/vsrvr1/vol3	/cls1-01/nrst01	clus1-01
2	Backup	COMPLETED	50MB	/vsrvr1/vol2	/cls1-03/nrst0m	clus1-03
1	Backup	COMPLETED	50KB	/vsrvr1/vol5	/cls1-01/nrst0n	clus1-01

5 entries were displayed.

The following example shows the output with the `-instance` argument.

---

```
cluster::> system smtape status show -instance
```

```
Session Identifier: 1
  Node Name: nodel
  Operation Type: Backup
  Status: COMPLETED
  Path Name: /vsl/voll
  Device Name: /nodel/rst0a
Bytes Transferred: 2048
  Start Time: 1/4/2012 14:26:24
  End Time: 1/4/2012 14:29:45
  Last updated: 1/4/2012 14:29:45
  Snapshot Name: voll.snapshot
  Tape Block Size: 240
Error Description: None
```

---

## system snmp authtrap

Enables or disables SNMP authentication traps

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Use this command to either enable or disable the standard SNMP authentication failure traps.

### Parameters

**[-authtrap <integer>]** - Enables SNMP Authentication Trap

Enter the value of 1 to enable SNMP authentication failure traps. By default, SNMP authentication trap is disabled and the value is 0.

### Examples

The following example demonstrates how to set the SNMP authtrap.

```
cluster1:> system snmp authtrap -authtrap 1
cluster1:> system snmp show
contact:
  private
location:
  NB
authtrap:
  1
init:
  0
traphosts:
  _
community:
  _
```

---

## system snmp contact

Displays or modifies contact details

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Sets the contact name as the System.sysContact.0 MIB-II variable.

### Parameters

**[-contact <text>]** - Contact

Specifies the contact name. Without any value specified, this command displays current setting of contact name.

### Examples

The following example sets the contact name for SNMP.

```
cluster1:> system snmp contact -contact private
cluster1:> system snmp show
contact:
  private
location:
  NB
authtrap:
  1
init:
  0
traphosts:
community:
  _
```

---

## system snmp init

Enables or disables SNMP traps

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Initializes or disables sending of traps by the SNMP daemon from the cluster.

### Parameters

**[-init <integer>]** - Initialize Traps

Use the value of 1 to initialize SNMP daemon to send traps or use a value of 0 to stop sending traps from the cluster. If no value is specified, this command displays the current setting of init. Traps are enabled by default.

### Examples

The following command initializes SNMP daemon to send traps.

```
cluster1:> system snmp init -init 1
cluster1:> system snmp show
contact:
  private
location:
  NB
authtrap:
  1
init:
  1
traphosts:
  _
community:
  _
```

## system snmp location

Displays or modifies location information

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description



---

Sets the location name as the System.sysLocation.0 MIB-II variable.

## Parameters

**[-location <text>]** - Location

Specifies the location details. If no value is specified, this command displays the current setting of location.

## Examples

This command sets the location name.

```
cluster1::> system snmp location -location NB
cluster1::> system snmp show
contact:
  private
location:
  NB
authtrap:
  1
init:
  1
traphosts:
  _
community:
  _
```

---

## system snmp show

Displays SNMP settings

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Lists the current values of all the parameters.

### Parameters

None

### Examples

```
cluster1::>system snmp show
contact:
location: private
authtrap: NB
init: 1
traphosts: 1
community: xxx.example.com(192.168.xxx.xxx)
community: _ _
```

---

## system snmp community add

Adds a new community with the specified access control type

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Adds communities with the specified access control type. Only read-only communities are supported. There is no limit for the number of communities supported.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which to add the community.

**-community-name** <text> - Community

Specifies the name of the community.

**-type** <ctype> - access type

Specifies 'ro' for read-only community.

### Examples

The following command adds the read-only community name 'private'.

```
cluster1::> system snmp community add -type ro
              -community-name private
Or
cluster1::> system snmp community add ro private
cluster1::> system snmp community show
              ro    private
```

---

## system snmp community delete

Deletes community with the specified access control type

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Deletes communities with the specified access control type. Only read-only communities are supported.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which to delete the community.

**-community-name** <text> - Community

Specify the name of the community.

**-type** <ctype> - access type

Specify 'ro' for a read-only community.

### Examples

This command deletes the read-only community 'private'.

```
cluster1::> system snmp community delete -type ro
               -community-name private
Or
cluster1::> system snmp community delete ro private
cluster1::> system snmp community show
This table is currently empty.
```

---

## system snmp community show

Displays communities

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Displays the current list of communities.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[**-vserver** <vserver name>] - Vserver

Use this parameter to specify the Vserver to which the SNMP community belongs

[**-community-name** <text>] - Community

Use this parameter to specify the SNMP v1/v2c community string

[**-access** <ctype>] - access

Use this parameter to specify the access type of the SNMP v1/v2c community. Read-only (ro) is the only access type supported

### Examples

```
cluster1::> system snmp community show
cluster1
      ro private
```

## system snmp traphost add

---

Add a new traphost

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

Adds SNMP managers who receive the SNMP trap PDUs. SNMP manager can be a hostname or IP address. There is no limit on the number of traphosts supported.

## Parameters

**-peer-address** <Remote InetAddress> - hostname|ipaddress

Specifies the IP address or hostname of the host.

## Examples

This command adds a new hostname 'yyy.example.com'.

```
cluster1::> system snmp traphost add -peer-address yyy.example.com
Or
cluster1::> system snmp traphost add yyy.example.com
cluster1::> system snmp traphost show
    yyy.example.com(yyy.example.com)(192.168.xxx.xxx)
    xxx.example.com(xxx.example.com)(xxx.xxx.xxx.xxx)
```

---

## system snmp traphost delete

Delete a traphost

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Deletes SNMP managers who receive SNMP trap PDUs. SNMP managers can be hostname or IP address. There is no limit on the number of traphosts supported.

### Parameters

**-peer-address** <Remote InetAddress> - hostname|ipaddress

Specifies the IP address or hostname of the host.

### Examples

This command deletes a traphost 'yyy.example.com'.

```
cluster1::> system snmp traphost delete -peer-address yyy.example.com
Or
cluster1::> system snmp traphost delete yyy.example.com
cluster1::> system snmp show
xxx.example.com(xxx.example.com)(xxx.xxx.xxx.xxx)
```

---

## system snmp traphost show

Displays traphosts

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Displays list of SNMP managers who receive trap PDUs.

### Parameters

None

### Examples

This command displays all host names or IP addresses that have been added till now.

```
cluster1::> system snmp traphost show
xxx.example.com(xxx.example.com) (xxx.xxx.xxx.xxx)
```

## system timeout modify

Set the CLI inactivity timeout value

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `system timeout modify` command sets the timeout value for CLI sessions. If there is no CLI activity during the length of the timeout interval, the logged in user is logged out. The default value is 30 minutes. To prevent CLI sessions from timing out, specify a value of 0 (zero).

### Parameters

**[-timeout <integer>]** - Timeout (in minutes)

Use this parameter to specify the timeout value, in minutes.



---

## Examples

The following example shows how to modify the timeout value for CLI sessions to be 10 minutes:

```
cluster1::> system timeout modify -timeout 10
```

The following example shows how to prevent CLI sessions from timing out:

```
cluster1::> system timeout modify -timeout 0
```

## system timeout show

Display the CLI inactivity timeout value

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `system timeout show` command displays the timeout value for CLI sessions. If there is no CLI activity during the length of the timeout interval, the logged in user is logged out. A timeout value of 0 minutes means that the CLI sessions never time out.

## Parameters

None

## Examples

The following example displays the timeout value for CLI sessions:

```
cluster1::> system timeout show
CLI session timeout: 15 minute(s)
```

---

## volume autosize

Set/Display the autosize settings of the flexible volume.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume autosize` command allows the user to specify the maximum size and increment that a volume will automatically grow to when it is out of space or the minimum size that it will shrink to when the amount of used space is below a certain threshold. If only the volume/Vserver name is specified then the current settings are displayed. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter can be used to specify the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This parameter specifies the volume for which the user wants to set or display the autosize configuration.

**[-maximum-size** {<integer>[KB|MB|GB|TB|PB]] - Maximum Autosize

This parameter allows the user to specify the maximum size to which a flexible volume can grow. The default for FlexVol volumes is 120% of the volume size. If the value of this parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the maximum size is reset to 120% of the volume size. The value for `-maximum-size` cannot be set larger than the platform-dependent maximum FlexVol volume size. If you specify a larger value, the value of `-maximum-size` is automatically reset to the supported maximum without returning an error. The default value for a FlexCache volume is the greater of either the origin volume's size or the current maximum size. This parameter is not supported on Infinite Volumes.

**[-increment-size** {<integer>[KB|MB|GB|TB|PB]] - Increment Size

When increasing the size of a volume, Data ONTAP uses the specified increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-maximum-size` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value

---

of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**[-increment-percent <percent>]** - Increment Percentage

The specified increment percent is converted to a fixed increment size in bytes based on the volume size when the command is issued. When increasing the size of a volume, Data ONTAP uses this computed increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-maximum-size` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**[-minimum-size {<integer>[KB|MB|GB|TB|PB]}]** - Minimum Autosize

This parameter specifies the minimum size to which the volume can automatically shrink. If the volume was created with the `grow_shrink` autosize mode enabled, then the default minimum size is equal to the initial volume size. If the value of the `-minimum-size` parameter is invalidated by a manual volume resize or is invalid when autosize is enabled, the minimum size is reset to the volume size. This parameter is not supported on Infinite Volumes.

**[-grow-threshold-percent <percent>]** - Grow Threshold Used Space Percentage

This parameter specifies the used space threshold for the automatic growth of the volume. When the volume's used space becomes greater than this threshold, the volume will automatically grow unless it has reached the maximum autosize. This parameter is not supported on Infinite Volumes.

**[-shrink-threshold-percent <percent>]** - Shrink Threshold Used Space Percentage

This parameter specifies the used space threshold for the automatic shrinking of the volume. When the amount of used space in the volume drops below this threshold, the volume will shrink unless it has reached the specified minimum size. This parameter is not supported on Infinite Volumes.

**{ [-mode {off|grow|grow\_shrink}]}** - Autosize Mode

This parameter specifies the autosize mode for the volume. The supported autosize modes are:

- `off` - The volume will not grow or shrink in size in response to the amount of used space.
- `grow` - The volume will automatically grow when used space in the volume is above the grow threshold.

- 
- `grow_shrink` - The volume will grow or shrink in size in response to the amount of used space.

By default, `-mode` is off for new FlexVol volumes, except for DP mirrors, for which the default value is `grow_shrink`. For FlexCache volumes created without specifying a size, the default value for `-mode` is `grow`. The `grow` and `grow_shrink` modes work together with Snapshot autodelete to automatically reclaim space when a volume is about to become full. The volume parameter `-space-mgmt-try-first` controls the order in which these two space reclamation policies are attempted. This parameter is not supported in Infinite Volumes.

| **`[-is-enabled {on|off}]`** - Autosize Enabled

Note that this option has been deprecated in Data ONTAP 8.2 and later. Use the `-mode` parameter instead. Volume autosize allows a FlexVol volume to automatically grow in size within an aggregate. By default `-is-enabled` is disabled for FlexVol volumes but is enabled for FlexCache volumes if a size is not specified upon creation. This option can be used to enable or disable autosize on a volume. Enabling this option is equivalent to setting `-mode` to `grow`, disabling the autoshrink functionality if it is currently enabled. This parameter cannot be specified with the `-mode` parameter. This parameter is not supported in Infinite Volumes.

**`[-reset [true]]`** - Autosize Reset

This option allows the user to reset the values of `autosize`, `autosize-increment`, `max-autosize`, `min-autosize`, `autosize-grow-threshold-percent`, `autosize-shrink-threshold-percent` and `autosize-mode` to their default values based on the current size of the volume. For example, the `max-autosize` value will be set to 120% of the current size of the volume.

## Examples

The following example sets the autosize settings on a volume named `vol1`. The maximum size to grow is 1TB, the increment is 10g and autogrow is enabled.

```
cluster::> vol autosize vol1 -maximum-size 1t -increment-size 10g -mode grow
(volume autosize)
vol autosize: Flexible volume 'vs1:vol1' autosize settings UPDATED.
```

The following example shows the autosize settings on a volume named `vol1`. The maximum size to grow is 1TB, the increment is 10g and autogrow is enabled.

```
cluster::> vol autosize vol1
(volume autosize)
Volume autosize is currently ON for volume 'vs1:vol1'.
The volume is set to grow to a maximum of 1t, in increments of 10g.
```

---

## volume create

Create a new volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume create` command creates a volume on a specified Vserver and storage aggregate. You can optionally specify the following attributes for the new volume:

- Size
- State (online, offline, restricted, or force-online)
- Type (read-write, data-protection, or data-cache)
- Export policy
- User ID
- Group ID
- Security style (Infinite Volume: Unified UNIX, NFS and CIFS permissions. All other volume types: UNIX mode bits, CIFS ACLs, or mixed NFS and CIFS permissions)
- Default UNIX permissions for files on the volume
- Language
- Junction path
- Whether the junction path is active (advanced privilege level or higher only)
- Whether the volume is the root volume for its Vserver (advanced privilege level or higher only)
- Comment
- Whether autosizing is enabled for FlexVols
- Maximum size for autosizing FlexVols
- Autosize increment for FlexVols
- Minimum size for autosize
- Grow used space threshold percentage for autosize
- Shrink used space threshold percentage for autosize

- 
- Whether autosizing is enabled for FlexVols
  - Current mode of operation of volume autosize
  - Maximum directory size (advanced privilege level or higher only)
  - Space guarantee style (none or volume)
  - Snapshot policy
  - Snapshot reserve percentage
  - Whether the volume create operation runs as a foreground or background process
  - FlexCache origin volume
  - FlexCache cache policy (advanced privilege level or higher only)

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the name of the volume that is to be created. A volume's name must start with an alphabetic character (a to z or A to Z) and be 150 or fewer characters in length for Infinite Volumes, and 203 or fewer characters in length for all other volume types. Volume names must be unique within a Vserver.

**-aggregate** <aggregate name> - Aggregate Name

This specifies the storage aggregate on which the volume is to be created. This parameter does not apply to Infinite Volumes.

**[-size** {<integer>[KB|MB|GB|TB|PB]] - Volume Size

This optionally specifies the size of the volume. The size is specified as a number followed by a unit designation: k (kilobytes), m (megabytes), g (gigabytes), or t (terabytes). If the unit designation is not specified, bytes are used as the unit, and the specified number is rounded up to the nearest 4 KB. The minimum size for a volume is 20 MB (the default setting). The volume's maximum size is limited by the platform maximum. If the volume's guarantee is set to `file` or `volume`, the volume's maximum size can also be limited by the available space in the hosting aggregate. Volumes can be increased and decreased in size with the `volume modify` command. If this is not specified for a FlexCache volume, the default size is 1 KB times the maximum number of files the source volume is currently configured for. The maximum number of files a

---

volume is configured for is listed under "Total Files" when running the command `volume show -instance`.

**[-state {online|restricted|offline|force-online|force-offline|mixed}]** - Volume State

This optionally specifies the volume's state. A restricted volume does not provide client access to data but is available for administrative operations.

Note:

The mixed state applies to Infinite Volumes only and cannot be specified as a target state.

**[-type {RW|DP|DC}]** - Volume Type

This optionally specifies the volume's type, either read-write, data-protection, or data-cache. If you do not specify a value for this parameter, a read-write volume is created by default. If you specify a FlexCache origin volume, a data-cache volume is created by default.

**[-policy <text>]** - Export Policy

This optionally specifies the ID number of the export policy associated with the volume. For information on export policies, see the documentation for the `vserver export-policy create` command.

**[-user <user name>]** - User ID

This optionally specifies the name or ID of the user that is set as the owner of the volume's root.

**[-group <group name>]** - Group ID

This optionally specifies the name or ID of the group that is set as the owner of the volume's root.

**[-security-style {unix|ntfs|mixed|unified}]** - Security Style

This optionally specifies the security style for the volume. Possible values include `unix` (for UNIX mode bits), `ntfs` (for CIFS ACLs), `mixed` (for mixed NFS and CIFS permissions) and `unified` (for mixed NFS and CIFS permissions with unified ACLs). Regardless of the security style, both NFS and CIFS clients can read from and write to the volume. Infinite Volumes support the unified security style only, and the unified security style can only be used on Infinite Volumes.

**[-unix-permissions <unix perm>]** - UNIX Permissions

This optionally specifies the default UNIX permissions for files on the volume. Specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of

---

the UNIX `ls` command (for example, `-rwxr-x---`). For information on UNIX permissions, see the UNIX or Linux documentation. The default setting is 0755 or `---rwxr-xr-x`.

**`[-junction-path <junction path>]`** - Junction Path

This optionally specifies the volume's junction path. The junction path name is case insensitive and must be unique within a Vserver's namespace.

**`[-junction-active {true|false}]`** - Junction Active (privilege: advanced)

This optionally specifies whether the volume's junction path is active. The default setting is `true`. If the junction path is inactive, the volume does not appear in the Vserver's namespace. This parameter is available only at the advanced privilege level and higher.

**`[-vsroot {true|false}]`** - Vserver Root Volume (privilege: advanced)

This optionally specifies whether the volume is the root volume of its Vserver. The default setting is `false`. If this parameter is set to `true`, the default size of the newly created volume is 1GB. This parameter is not supported on Infinite Volumes.

**`[-comment <text>]`** - Comment

This optionally specifies a comment for the volume.

**`[-max-autosize {<integer>[KB|MB|GB|TB|PB]}]`** - Maximum Autosize (for flexvols only)

This parameter allows the user to specify the maximum size to which a flexible volume can grow. The default for FlexVol volumes is 120% of the volume size. If the value of this parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the maximum size is reset to 120% of the volume size. The value for `-max-autosize` cannot be set larger than the platform-dependent maximum FlexVol volume size. If you specify a larger value, the value of `-max-autosize` is automatically reset to the supported maximum without returning an error. The default value for a FlexCache volume is the greater of either the origin volume's size or the current maximum size. This parameter is not supported on Infinite Volumes.

**`[-autosize-increment | -i {<integer>[KB|MB|GB|TB|PB]}]`** - Autosize Increment (for flexvols only)

When increasing the size of a volume, Data ONTAP uses the specified increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-max-autosize` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**`[-autosize-increment-percent | -p <percent>]`** - Autosize Increment Percent (for flexvols only)



---

The specified increment percent is converted to a fixed increment size in bytes based on the volume size when the command is issued. When increasing the size of a volume, Data ONTAP uses this computed increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-max-autosize` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**`[-min-autosize {<integer>[KB|MB|GB|TB|PB]]`** - Minimum Autosize

This parameter specifies the minimum size to which the volume can automatically shrink. If the volume was created with the `grow_shrink` autosize mode enabled, then the default minimum size is equal to the initial volume size. If the value of the `-min-autosize` parameter is invalidated by a manual volume resize or is invalid when autosize is enabled, the minimum size is reset to the volume size. This parameter is not supported on Infinite Volumes.

**`[-autosize-grow-threshold-percent <percent>]`** - Autosize Grow Threshold Percentage

This parameter specifies the used space threshold for the automatic growth of the volume. When the volume's used space becomes greater than this threshold, the volume will automatically grow unless it has reached the maximum autosize. This parameter is not supported on Infinite Volumes.

**`[-autosize-shrink-threshold-percent <percent>]`** - Autosize Shrink Threshold Percentage

This parameter specifies the used space threshold for the automatic shrinking of the volume. When the amount of used space in the volume drops below this threshold, the volume will shrink unless it has reached the specified minimum size. This parameter is not supported on Infinite Volumes.

**`{ [-autosize-mode {off|grow|grow_shrink}]`** - Autosize Mode

This parameter specifies the autosize mode for the volume. The supported autosize modes are:

- `off` - The volume will not grow or shrink in size in response to the amount of used space.
- `grow` - The volume will automatically grow when used space in the volume is above the grow threshold.
- `grow_shrink` - The volume will grow or shrink in size in response to the amount of used space.

---

By default, `-autosize-mode` is off for new FlexVol volumes, except for DP mirrors, for which the default value is `grow_shrink`. For FlexCache volumes created without specifying a size, the default value of `-autosize-mode` is `grow`. The `grow` and `grow_shrink` modes work together with Snapshot autodelete to automatically reclaim space when a volume is about to become full. The volume parameter `-space-mgmt-try-first` controls the order in which these two space reclamation policies are attempted. This parameter is not supported in Infinite Volumes.

| **[-autosize {true|false}]** } - Autosize Enabled (for flexvols only)

Note that this option has been deprecated in Data ONTAP 8.2 and later. Use the `-autosize-mode` parameter instead. Volume autosize allows a FlexVol volume to automatically grow in size within an aggregate. By default `-autosize` is disabled for FlexVol volumes but is enabled for FlexCache volumes if a size is not specified upon creation. This option can be used to enable or disable autosize on a volume. Enabling this option is equivalent to setting `-autosize-mode` to `grow`, disabling the autoshrink functionality if it is currently enabled. This parameter cannot be specified with the `-autosize-mode` parameter. This parameter is not supported in Infinite Volumes.

**[-maxdir-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Directory Size (privilege: advanced)

This optionally specifies the maximum directory size. The default setting is 102,400 KB (or 100 MB). This parameter is available only at the advanced privilege level and higher. This parameter is not supported on Infinite Volumes.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

This optionally specifies the space-reservation policy for the volume. A value of `volume` reserves space on the aggregate for the entire volume. A value of `none` reserves no space on the aggregate, meaning that writes can fail if the aggregate runs out of space; because CIFS does not handle out-of-space conditions, do not use this value if the volume is accessible to CIFS clients. The default setting is `volume`. Infinite Volumes support the `none` and `volume` space-reservation policies only.

**[-percent-snapshot-space <percent>]** - Space Reserved for Snapshots

This optionally specifies the amount of space that is reserved in the volume for Snapshots. The default setting is 5 percent.

**[-snapshot-policy <snapshot policy>]** - Snapshot Policy

This optionally specifies the Snapshot policy for the volume. The default is the Snapshot policy for all volumes on the Vserver, as specified by the `-snapshot-policy` parameter of the `vserver create` and `vserver modify` commands. The schedules associated with the `snapshot-policy` for an Infinite Volume cannot have an interval shorter than hourly.

---

**[-language <Language code>]** - Language

This optionally specifies the language encoding setting for the volume. By default, the volume inherits the Vserver language encoding setting. You cannot specify the language encoding setting for an Infinite Volume.

Note:

You cannot modify the language encoding setting of a volume.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

**[-antivirus-on-access-policy <antivirus policy>]** - Antivirus On-Access Policy

This optionally specifies which antivirus on-access policy to apply to the volume. For more information on the antivirus on-access policies see the `antivirus on-access policy show` command. The default setting is the antivirus on-access policy which is set for the Vserver on which the volume is being created. This parameter is not supported on Infinite Volumes.

**[-flexcache-cache-policy <cache policy>]** - FlexCache Cache Policy (privilege: advanced)

This optionally specifies which FlexCache cache policy to apply to the volume. If this is not specified, the default cache policy for the Vserver is used. This parameter is available only at advanced privilege level and higher. This parameter is not supported on Infinite Volumes.

**[-flexcache-min-reserve {<integer>[KB|MB|GB|TB|PB]}]** - FlexCache Minimum Reserve (privilege: advanced)

This optionally specifies the amount of space requested to be preallocated in the aggregate hosting the FlexCache volume. This parameter is not supported on Infinite Volumes.

**[-nvfail {on|off}]** - NVFAIL Option

Setting this optional parameter to `true` causes the volume to set the `in-nvfailed-state` flag to `true`, if committed writes to the volume are lost due to a failure. The `in-nvfailed-state` flag fences the volume from further data access and prevents possible corruption of the application data. Without specifying a value, this parameter is automatically set to `false`.

**[-flexcache-origin-volume <volume name>]** - FlexCache Origin Volume Name

---

If the volume type is data-cache, this mandatory parameter specifies the data-protection or read-write volume that contains the authoritative data for this data-cache volume. This parameter is not supported on Infinite Volumes.

**[-enable-snapdiff {true|false}]** - Create Namespace Mirror Constituents For SnapDiff Use

When set to true for an Infinite Volume that spans three or more nodes, namespace mirror constituents are created for SnapDiff use. One namespace mirror constituent is created on every node that contains a data constituent for the Infinite Volume. A namespace constituent is not created on nodes that contain either the namespace constituent or a namespace mirror constituent used for data protection of the namespace constituent. An automatic daily replication schedule is set up for every namespace mirror constituent created. The default setting is false. This parameter applies to Infinite Volumes only.

**[-unreachable-attr-action {return-generated|wait}]** - Action When Attributes Are Not Reachable (privilege: advanced)

This parameter specifies the information that an Infinite Volume returns when a client lists a directory that contains one or more files with inaccessible attributes, which can happen when a data constituent is not online. When this parameter is set to return-generated, the Infinite Volume returns default values for the attributes, which appear to the client as a file size of 0 and timestamps that are in the past. When this parameter is set to wait, the Infinite Volume returns a RETRY error, which may cause some clients to hang. When the inaccessible file attributes become available, the Infinite Volume returns them to the client. The default setting is return-generated. This parameter is not supported for FlexVol volumes.

**[-namespace-aggregate <aggregate name>]** - Namespace Aggregate (privilege: advanced)

The name of the aggregate in which to create the Infinite Volume namespace constituent. If not provided, ONTAP will pick the best available aggregate assigned to the Vserver. This parameter applies to Infinite Volumes only.

**[-max-namespace-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Namespace Constituent (privilege: advanced)

The maximum size of the namespace constituent. The default value is 10TB. This parameter applies to Infinite Volumes only.

**[-ns-mirror-aggr-list <aggregate name>, ...]** - List of Aggregates for Namespace Mirrors (privilege: advanced)

Specifies the aggregates that can be used to create Infinite Volume namespace mirror constituents. No other aggregate will be chosen for this purpose. Aggregates in this

---

list will remain available for other uses in the Infinite Volume. This parameter applies to Infinite Volumes only.

**[-data-aggr-list <aggregate name>, ...]** - List of Aggregates for Data Constituents (privilege: advanced)

Specifies the aggregates that can be used to create Infinite Volume data constituents. No other aggregate will be chosen for this purpose. Aggregates in this list will remain available for other uses in the Infinite Volume. This parameter applies to Infinite Volumes only.

**[-max-data-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Each Data Constituent (privilege: advanced)

This optional parameter specifies the maximum size of an Infinite Volume data constituent. The default value is determined by checking the maximum FlexVol size setting on all nodes used by the Infinite Volume. The smallest value found is chosen as the default for the `max-data-constituent-size` for the Infinite Volume. This parameter applies to Infinite Volumes only.

**[-qos-policy-group <text>]** - QoS Policy Group Name

This optionally specifies which QoS policy group to apply to the volume. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a volume, the system will not monitor and control the traffic to it. This parameter is not supported on Infinite Volumes.

## Examples

The following example creates a new volume named `user_jdoe` on a Vserver named `vs0` and a storage aggregate named `aggr1`. Upon its creation, the volume is placed in the online state. It uses the export policy named `default_expolicy`. The owner of the volume's root is a user named `jdoe` whose primary group is named `dev`. The volume's junction path is `/user/jdoe`. The volume is 250 GB in size, space for the entire volume is reserved on the aggregate, and the create operation runs in the background.

```
node::> volume create -vserver vs0 -volume user_jdoe -aggregate aggr1 -state
online
                        -policy default_expolicy -user jdoe -group dev -junction-path /user/
jdoe -size 250g
-space-guarantee volume -percent-snapshot-space 20 -foreground false
```

## See Also

`volume modify` `volume show` `vserver export-policy create` `vserver create`  
`vserver modify` `antivirus on-access policy show`

---

## volume delete

Delete an existing volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume delete` command deletes the specified volumes. Before deleting a volume, the user is prompted to confirm the operation unless the `-force` flag is specified. If this volume was associated with a policy group the underlying qos workload is deleted.

Note:

If there is a qtree or quota policy associated with a volume, it is deleted when you delete the volume.

Note:

A volume must be offline (see `volume offline`) to be deleted.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver from which the volume is to be deleted. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the name of the volume that is to be deleted.

**[-force [true]]** - Force Delete (privilege: advanced)

If this parameter is specified, the user is not prompted to confirm each deletion operation. In addition, the operation is run only on the local node, and several potential errors are ignored. By default, this setting is `false`. This parameter is available only at the advanced privilege level and higher.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return

---

until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

## Examples

The following example deletes a volume named vol1\_old from a Vserver named vs0:

```
cluster::> volume delete -vserver vs0 -volume vol1_old
```

## See Also

volume offline

---

## volume make-vsroot

Designate a non-root volume as a root volume of the Vserver

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `volume make-vsroot` command promotes a non-root volume of the Vserver to be the Vserver's root volume. The Vserver's root volume must be a FlexVol volume. This command is not supported on Infinite Volumes. For instance, if you run this command on a volume named `user` that is located on a Vserver named `vs0`, the volume `user` is made the root volume of the Vserver `vs0`.

This command is available only at the advanced privilege level and higher.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which a non-root volume is to be made the root volume.

**-volume** <volume name> - Volume Name

This specifies the non-root volume that is to be made the root volume of its Vserver.

### Examples

The following example makes a volume named `root_vs0_backup` the root volume of its Vserver, which is named `vs0`.

```
node::> volume make-vsroot -vserver vs0 -volume root_vs0_backup
```

## volume modify

Modify volume attributes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description



---

The `volume modify` command can be used to modify the following attributes of a volume:

- Size
- State (online, offline, restricted, force-online or force-offline)
- Export policy
- User ID
- Group ID
- Security style (Infinite Volume: Unified UNIX, NFS and CIFS permissions. All other volume types: UNIX mode bits, CIFS ACLs, or mixed NFS and CIFS permissions)
- Default UNIX permissions for files on the volume
- Whether the junction path is active
- Comment
- Volume nearly full threshold percent
- Volume full threshold percent
- Maximum size for autosizing
- Autosize increment
- Minimum size for autosize
- Grow used space threshold percentage for autosize
- Shrink used space threshold percentage for autosize
- Whether autosizing is enabled
- Current mode of operation of volume autosize
- Reset the autosize values to their defaults
- Total number of files for user-visible data permitted on the volume
- Space guarantee style (none, file or volume)
- Snapshot policy
- Convert ucode
- FlexCache cache policy

---

You can use the `volume move` command to change a volume's aggregate or node. You can use the `volume rename` command to change a volume's name. You can use the `volume make-vsroot` command to make a volume the root volume of its Vserver.

You can change additional volume attributes by using this command at the advanced privilege level and higher.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the volume that is to be modified.

**[-size** {<integer>[KB|MB|GB|TB|PB]]} - Volume Size

This optionally specifies the new size of the volume. The size is specified as a number followed by a unit designation: k (kilobytes), m (megabytes), g (gigabytes), or t (terabytes). If the unit designation is not specified, bytes are used as the unit, and the specified number is rounded up to the nearest 4 KB. A relative rather than absolute size change can be specified by adding + or - before the given size: for example, specifying +30m adds 30 megabytes to the volume's current size. The minimum size for a volume is 20 MB (the default setting). The volume's maximum size is limited by the platform maximum. If the volume's guarantee is set to `file` or `volume`, the volume's maximum size can also be limited by the available space in the hosting aggregate. If the volume's guarantee is currently disabled, its size cannot be increased. This parameter is not supported on Infinite Volumes that are managed by storage services.

**[-state** {online|restricted|offline|force-online|force-offline|mixed}] - Volume State

This optionally specifies the volume's state. A restricted volume does not provide client access to data but is available for administrative operations.

Note:

The mixed state applies to Infinite Volumes only and cannot be specified as a target state.

**[-policy** <text>] - Export Policy

This optionally specifies the ID number of the export policy associated with the volume. For information on export policy, see the documentation for the `vserver export-policy create` command.

---

**[-user <user name>]** - User ID

This optionally specifies the name or ID of the user that is set as the owner of the volume's root.

**[-group <group name>]** - Group ID

This optionally specifies the name or ID of the group that is set as the owner of the volume's root.

**[-security-style {unix|ntfs|mixed|unified}]** - Security Style

This optionally specifies the security style for the volume. Possible values include `unix` (for UNIX mode bits), `ntfs` (for CIFS ACLs), `mixed` (for mixed NFS and CIFS permissions) and `unified` (for mixed NFS and CIFS permissions with unified ACLs). Regardless of the security style, both NFS and CIFS clients can read from and write to the volume. Infinite Volumes support the unified security style only, and the unified security style can only be used on Infinite Volumes.

**[-unix-permissions <unix perm>]** - UNIX Permissions

This optionally specifies the default UNIX permissions for files on the volume. Specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX `ls` command (for example, `-rwxr-x---`). For information on UNIX permissions, see the UNIX or Linux documentation. The default setting is 0755 or `-rwxr-xr-x`.

**[-junction-active {true|false}]** - Junction Active (privilege: advanced)

This optionally specifies whether the volume's junction path is active. The default setting is `true`. If the junction is inactive, the volume does not appear in the Vserver's namespace.

**[-comment <text>]** - Comment

This optionally specifies a comment for the volume.

**[-space-nearly-full-threshold-percent <percent>]** - Volume Nearly Full Threshold Percent

This optionally specifies the percentage at which the volume is considered nearly full, and above which an EMS warning will be generated. This parameter is not supported on Infinite Volumes. The default value is 95%. The maximum value for this option is 99%. Setting this threshold to 0 disables the volume nearly full space alerts.

**[-space-full-threshold-percent <percent>]** - Volume Full Threshold Percent

This optionally specifies the percentage at which the volume is considered full, and above which a critical EMS error will be generated. This parameter is not supported on Infinite Volumes. The default value is 98%. The maximum value for this option is 100%. Setting this threshold to 0 disables the volume full space alerts.

---

**[-max-autosize {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Autosize (for flexvols only)

This parameter allows the user to specify the maximum size to which a flexible volume can grow. The default for FlexVol volumes is 120% of the volume size. If the value of this parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the maximum size is reset to 120% of the volume size. The value for `-max-autosize` cannot be set larger than the platform-dependent maximum FlexVol volume size. If you specify a larger value, the value of `-max-autosize` is automatically reset to the supported maximum without returning an error. The default value for a FlexCache volume is the greater of either the origin volume's size or the current maximum size. This parameter is not supported on Infinite Volumes.

**[-autosize-increment | -i {<integer>[KB|MB|GB|TB|PB]}]** - Autosize Increment (for flexvols only)

When increasing the size of a volume, Data ONTAP uses the specified increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-max-autosize` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**[-autosize-increment-percent | -p <percent>]** - Autosize Increment Percent (for flexvols only)

The specified increment percent is converted to a fixed increment size in bytes based on the volume size when the command is issued. When increasing the size of a volume, Data ONTAP uses this computed increment as a guide; the actual size increase may be larger or smaller. The default is the lesser value of either 1GB or 5% of the volume size at the time the volume was created. If the value of the `-max-autosize` parameter is invalidated by manually resizing the volume or is invalid when the autosize feature is enabled, the increment is reset to the lesser value of either 1GB or 5% of the volume size. This parameter is not supported on Infinite Volumes.

**[-min-autosize {<integer>[KB|MB|GB|TB|PB]}]** - Minimum Autosize

This parameter specifies the minimum size to which the volume can automatically shrink. If the volume was created with the `grow_shrink` autosize mode enabled, then the default minimum size is equal to the initial volume size. If the value of the `-min-autosize` parameter is invalidated by a manual volume resize or is invalid when autosize is enabled, the minimum size is reset to the volume size. This parameter is not supported on Infinite Volumes.

**[-autosize-grow-threshold-percent <percent>]** - Autosize Grow Threshold Percentage

---

This parameter specifies the used space threshold for the automatic growth of the volume. When the volume's used space becomes greater than this threshold, the volume will automatically grow unless it has reached the maximum autosize. This parameter is not supported on Infinite Volumes.

**[-autosize-shrink-threshold-percent <percent>]** - Autosize Shrink Threshold Percentage

This parameter specifies the used space threshold for the automatic shrinking of the volume. When the amount of used space in the volume drops below this threshold, the volume will shrink unless it has reached the specified minimum size. This parameter is not supported on Infinite Volumes.

**{ [-autosize-mode {off|grow|grow\_shrink}]}** - Autosize Mode

This parameter specifies the autosize mode for the volume. The supported autosize modes are:

- off - The volume will not grow or shrink in size in response to the amount of used space.
- grow - The volume will automatically grow when used space in the volume is above the grow threshold.
- grow\_shrink - The volume will grow or shrink in size in response to the amount of used space.

By default, `-autosize-mode` is off for new flexible volumes, except for DP mirrors, for which the default value is `grow_shrink`. For FlexCache volumes created without specifying a size, the default value of `-autosize-mode` is `grow`. The `grow` and `grow_shrink` modes work together with Snapshot autodelete to automatically reclaim space when a volume is about to become full. The volume parameter `-space-mgmt-try-first` controls the order in which these two space reclamation policies are attempted. This parameter is not supported in Infinite Volumes.

**| [-autosize {true|false}]** - Autosize Enabled (for flexvols only)

Note that this option has been deprecated in Data ONTAP 8.2 and later. Use the `-autosize-mode` parameter instead. Volume autosize allows a FlexVol volume to automatically grow in size within an aggregate. By default `-autosize` is disabled for FlexVol volumes but is enabled for FlexCache volumes if a size is not specified upon creation. This option can be used to enable or disable autosize on a volume. Enabling this option is equivalent to setting `-autosize-mode` to `grow`, disabling the autoshrink functionality if it is currently enabled. This parameter cannot be specified with the `-autosize-mode` parameter. This parameter is not supported in Infinite Volumes.

**[-autosize-reset [true]]** - Autosize Reset

---

This allows the user to reset the values of `autosize`, `autosize-increment`, `max-autosize`, `min-autosize`, `autosize-grow-threshold-percent`, `autosize-shrink-threshold-percent` and `autosize-mode` to their default values. For example, the `max-autosize` value will be set to 120% of the current size of the volume.

**[-files <integer>]** - Total Files (for user-visible data)

This optionally specifies the total number of files for user-visible data permitted on the volume. This value can be raised or lowered. Raising the total number of files does not immediately cause additional disk space to be used to track files. Instead, as more files are created on the volume, the system dynamically increases the number of disk blocks that are used to track files. The space assigned to track files is never freed, and the `files` value cannot be decreased below the current number of files that can be tracked within the assigned space for the volume.

**[-maxdir-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Directory Size (privilege: advanced)

This optionally specifies the maximum directory size. The default maximum directory size is model-dependent, and optimized for the size of system memory. You can increase it for a specific volume by using this option, but doing so could impact system performance. If you need to increase the maximum directory size, work with customer support. This parameter is not supported on Infinite Volumes.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

This option controls whether the volume is guaranteed some amount of space in the aggregate. The default is `volume`, and `file` and `none` can be set by the administrator. Infinite Volumes support the `none` and `volume` space-reservation policies only. `Volume guaranteed` means that the entire size of the volume is preallocated. The `file` value means that space is preallocated for all the space-reserved files and LUNs within the volume. Storage is not preallocated for files and LUNs that are not space-reserved. Writes to these can fail if the underlying aggregate has no space available to store the written data. This value can be set if fractional reserve is 100. The `none` value means that no space is preallocated, even if the volume contains space-reserved files or LUNs; if the aggregate is full, space is not available even for space-reserved files and LUNs within the volume. Setting this parameter to `file` or `none` enables you to provision more storage than is physically present in the aggregate (thin provisioning). When you use thin provisioning for a volume, it can run out of space even if it has not yet consumed its nominal size and you should carefully monitor space utilization to avoid unexpected errors due to the volume running out of space. For flexible root volumes, to ensure that system files, log files, and cores can be saved, the `space-guarantee` must be `volume`. This is to ensure support of the appliance by customer support, if a problem occurs. Disk space is preallocated when the volume is brought online and, if not used, returned to the aggregate when the volume is brought offline. It is possible to bring a volume online even when the aggregate has insufficient free space to preallocate to the volume.

---

In this case, no space is preallocated, just as if the none option had been selected. In this situation, the vol options and vol status command display the actual value of the space-guarantee option, but indicate that it is disabled. This parameter is not supported on Infinite Volumes that are managed by storage services.

**[-min-readahead {true|false}]** - Minimum Read Ahead (privilege: advanced)

This optionally specifies whether minimum readahead is used on the volume. The default setting is `false`.

**[-atime-update {true|false}]** - Access Time Update Enabled (privilege: advanced)

This optionally specifies whether the access time on inodes is updated when a file is read. The default setting is `true`.

**[-snapdir-access {true|false}]** - Snapshot Directory Access Enabled

This optionally specifies whether clients have access to .snapshot directories. The default setting is `true`.

**[-percent-snapshot-space <percent>]** - Space Reserved for Snapshots

This optionally specifies the amount of space that is reserved on the volume for Snapshot copies. The default setting is 5 percent.

**[-snapshot-policy <snapshot policy>]** - Snapshot Policy

This optionally specifies the Snapshot policy for the volume. The default is the Snapshot policy for all volumes on the Vserver, as specified by the `-snapshot-policy` parameter of the `vserver create` and `vserver modify` commands. The schedules associated with the `snapshot-policy` for an Infinite Volume cannot have an interval shorter than hourly.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

**[-antivirus-on-access-policy <antivirus policy>]** - Antivirus On-Access Policy

This optionally specifies which antivirus on-access policy to apply to the volume. This parameter is not supported on Infinite Volumes. For more information on the antivirus on-access policies see the `antivirus on-access policy show` command.

**[-flexcache-cache-policy <cache policy>]** - FlexCache Cache Policy (privilege: advanced)

This optionally specifies which FlexCache cache policy to apply to the volume. This parameter is not supported on Infinite Volumes.

---

**[-flexcache-min-reserve {<integer>[KB|MB|GB|TB|PB]}]** - FlexCache Minimum Reserve (privilege: advanced)

This optionally specifies the amount of space requested to be preallocated in the aggregate hosting the FlexCache volume. This parameter is not supported on Infinite Volumes.

**[-nvfail {on|off}]** - NVFAIL Option

Setting this optional parameter to true causes the volume to set the in-nvfailed-state flag to true, if committed writes to the volume are lost due to a failure. The in-nvfailed-state flag fences the volume from further data access and prevents possible corruption of the application data. Without specifying a value, this parameter is automatically set to false.

**[-in-nvfailed-state {true|false}]** - Volume's Nvfailed State (privilege: advanced)

This field is automatically set to true on a volume when committed writes to the volume are possibly lost due to a failure, and the volume has the nvfail option enabled. With this field set, the client access to the volume is fenced to protect against possible corruptions that result from accessing stale data. The administrator needs to take appropriate recovery actions to recover the volume from the possible data loss. After the recovery is completed, the administrator can clear this field and restore the client access to the volume. This field can be cleared using the CLI but it cannot be set.

**[-filesystems-size-fixed {true|false}]** - Is File System Size Fixed

This option causes the file system to remain the same size and not grow or shrink when a SnapMirrored volume relationship is broken, or when a volume add is performed on it. It is automatically set to true when a volume becomes a SnapMirrored volume. It stays set to true after the snapmirror break command is issued for the volume. This allows a volume to be SnapMirrored back to the source without needing to add disks to the source volume. If the volume is a traditional volume and the size is larger than the file system size, setting this option to false forces the file system to grow to the size of the volume. If the volume is a flexible volume and the volume size is larger than the file system size, setting this option to false forces the volume size to equal the file system size. The default setting is false.

**[-extent-enabled {off|on|space-optimized}]** - Extent Option

Setting this option to `on` or `space-optimized` enables extents in the volume. This causes application writes to be written in the volume as a write of a larger group of related data blocks called an extent. Using extents may help workloads that perform many small random writes followed by large sequential reads. However, using extents may increase the amount of disk operations performed on the controller, so this option should only be used where this trade-off is desired. If the option is set to `space-optimized` then the reallocation update will not duplicate blocks from Snapshot copies into the active file system, and will result in conservative space utilization. Using



---

`space-optimized` may be useful when the volume has Snapshot copies or is a SnapMirror source, when it can reduce the storage used in the volume and the amount of data that SnapMirror needs to move on the next update. The `space-optimized` value can result in degraded read performance of Snapshot copies. The default value is `off`; extents are not used.

**`[-fractional-reserve <percent>]` - Fractional Reserve**

This option changes the amount of space reserved for overwrites of reserved objects (LUNs, files) in a volume. This parameter is not supported on Infinite Volumes. The option is set to 100 by default with `guarantee` set to `volume` or `file`. A setting of 100 means that 100% of the required reserved space is actually reserved so the objects are fully protected for overwrites. The value is set to 0 by default with `guarantee` set to `none`. The value can be either 0 or 100 when `guarantee` is set to `volume` or `none`. If `guarantee` is set to `file`, 100 is the only allowed value. Using a value of 0 indicates that no space will be reserved for overwrites. This returns the extra space to the available space for the volume, decreasing the total amount of space used. However, this does leave the protected objects in the volume vulnerable to out of space errors. If the percentage is set to 0%, the administrator must monitor the space usage on the volume and take corrective action.

**`[-snapshot-clone-dependency {on|off}]` - Snapshot Cloning Dependency**

If set to `on`, LUN clone dependency on Snapshot copies is enabled. This parameter is not supported on Infinite Volumes.

**`[-space-mgmt-try-first {volume_grow|snap_delete}]` - Primary Space Management Strategy**

A flexible volume can be configured to automatically reclaim space in case the volume is about to run out of space, by either increasing the size of the volume using `autogrow` or deleting Snapshot copies in the volume using `Snapshot autodelete`. If this option is set to `volume_grow` the system will try to first increase the size of volume before deleting Snapshot copies to reclaim space. If the option is set to `snap_delete` the system will first automatically delete Snapshot copies and in case of failure to reclaim space will try to grow the volume. This parameter is not supported on Infinite Volumes.

**`[-read-realloc {off|on|space-optimized}]` - Read Reallocation Option**

Setting this option to `on` or `space-optimized` enables read reallocation in the volume. This results in the optimization of file layout by writing some blocks to a new location on disk. The layout is updated only after the blocks have been read because of a user read operation, and only when updating their layout will provide better read performance in the future. Using read reallocation may help workloads that perform a mixture of random writes and large sequential reads. If the option is set to `space-optimized` then the reallocation update will not duplicate blocks from Snapshot copies into the active file system, and will result in conservative space utilization. Using `space-optimized` may

---

be useful when the volume has Snapshot copies or is a SnapMirror source, when it can reduce the storage used in the volume and the amount of data that snapmirror needs to move on the next update. The `space-optimized` value can result in degraded read performance of Snapshot copies. The default value is `off`.

**[-enable-snapdiff {true|false}]** - Create Namespace Mirror Constituents For SnapDiff Use

When set to true for an Infinite Volume that spans three or more nodes, namespace mirror constituents are created for SnapDiff use. One namespace mirror constituent is created on every node that contains a data constituent for the Infinite Volume. A namespace mirror constituent is not created on nodes that contain either the namespace constituent or a namespace mirror constituent used for data protection of the namespace constituent. An automatic daily replication schedule is set up for every namespace mirror constituent created. If set to false, all existing namespace mirror constituents used by SnapDiff are deleted. The namespace mirror constituent used for namespace data protection is not affected. This parameter applies to Infinite Volumes only.

**[-unreachable-attr-action {return-generated|wait}]** - Action When Attributes Are Not Reachable (privilege: advanced)

This parameter specifies the information that an Infinite Volume returns when a client lists a directory that contains one or more files with inaccessible attributes, which can happen when a data constituent is not online. When this parameter is set to `return-generated`, the Infinite Volume returns default values for the attributes, which appear to the client as a file size of 0 and timestamps that are in the past. When this parameter is set to `wait`, the Infinite Volume returns a RETRY error, which may cause some clients to hang. When the inaccessible file attributes become available, the Infinite Volume returns them to the client. The default setting is `return-generated`. This parameter is not supported for FlexVol volumes.

**[-max-namespace-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Namespace Constituent (privilege: advanced)

The maximum size of the namespace constituent. The default value is 10TB. This parameter applies to Infinite Volumes only.

**[-ns-mirror-aggr-list <aggregate name>, ...]** - List of Aggregates for Namespace Mirrors (privilege: advanced)

Specifies the aggregates that can be used to create Infinite Volume namespace mirror constituents. No other aggregate will be chosen for this purpose. Aggregates in this list will remain available for other uses in the Infinite Volume. This parameter applies to Infinite Volumes only.

---

**[-max-data-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Each Data Constituent (privilege: advanced)

This parameter specifies the maximum size of an Infinite Volume data constituent. The default value is determined by checking the maximum FlexVol size setting on all nodes used by the Infinite Volume. The smallest value found is chosen as the default for the maximum constituent size. This parameter applies to Infinite Volumes only.

**[-qos-policy-group <text>]** - QoS Policy Group Name

This optionally specifies which QoS policy group to apply to the volume. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a volume, the system will not monitor and control the traffic to it. To remove this volume from a policy group, enter the reserved keyword "none". This parameter is not supported on Infinite Volumes.

## Examples

The following example modifies a volume named vol4 on a Vserver named vs0. The volume's export policy is changed to default\_expolicy and its size is changed to 500 GB.

```
cluster::> volume modify -vserver vs0 -volume vol4 -policy default_expolicy -size 500g
```

The following example modifies a volume named vol2. It enables autogrow and sets the maximum autosize to 500g and autosize increment to 20g

```
cluster::> volume modify -volume vol2 -autosize-mode grow -max-autosize 500g -autosize-increment 20g
```

The following example modifies a volume named vol2 to have an autosize increment of 50g

```
cluster::> volume modify -volume vol2 -autosize-increment 50g
```

The following example modifies a volume named vol2 to have a space guarantee of none.

```
cluster::> volume modify -space-guarantee none -volume vol2
```

The following example modifies all volumes in Vserver vs0 to have a fractional reserve of 30%.

```
cluster::> volume modify -fractional-reserve 30 -vserver vs0 *
```

The following example modifies a volume named vol2 to grow in size by 5 gigabytes

```
cluster::> volume modify -volume vol2 -size +5g
```

## See Also

---

vserver export-policy create vserver create vserver modify antivirus on-  
access policy show volume move volume rename volume make-vsroot

---

## volume mount

Mount a volume on another volume with a junction-path

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume mount` command mounts a volume at a specified junction path.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the volume that is to be mounted.

**-junction-path** <junction path> - Junction Path Of The Mounting Volume

This specifies the junction path of the mounted volume. The junction path name is case insensitive and must be unique within a Vserver's namespace.

**[-active {true|false}]** - Activate Junction Path

This optionally specifies whether the mounted volume is accessible. The default setting is `false`. If the mounted path is not accessible, it does not appear in the Vserver's namespace.

**[-policy-override {true|false}]** - Override The Export Policy

This optionally specifies whether the parent volume's export policy overrides the mounted volume's export policy. The default setting is `false`.

### Examples

The following example mounts a volume named `user_tsmith` on a Vserver named `vs0`. The junction path for the mounted volume is `/user/tsmith`. The mounted volume is accessible, and the mounted volume's export policy is not overridden by the parent volume's export policy.

```
node::> volume mount -vserver vs0 -volume user_tsmith  
-junction-path /user/tsmith -active true -policy-override false
```

---

## volume offline

Take an existing volume offline

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume offline` command takes the volume offline. If the volume is already in restricted or `iron_restricted` state, then it is already unavailable for data access, and much of the following description does not apply. The current root volume may not be taken offline. A number of operations being performed on the volume in question can prevent volume offline from succeeding for various lengths of time. If such operations are required, the command may take additional time to complete. If they do not, the command is aborted. The `-force` flag can be used to forcibly offline a volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver from which the volume is to be taken offline. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the name of the volume that is to be taken offline.

**[-force | -f [true]]** - Force Offline

This specifies whether the offline operation is forced. Using this option to force a volume offline can potentially disrupt access to other volumes. The default setting is `false`.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

### Examples

The following example takes the volume named `vol1` offline:

```
cluster:> volume offline vol1
Volume 'vs1:vol1' is now offline.
```

---

## volume online

Bring an existing volume online

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume online` command brings the volume online. A volume can only be brought online if it is offline or restricted. If the volume is inconsistent but has not lost data, the user will be cautioned and prompted before bringing it online. It is advisable to run `waf-iron` (or do a `snapmirror initialize` in case of a replica volume) prior to bringing an inconsistent volume online. Bringing an inconsistent volume online increases the risk of further file system corruption. If the containing aggregate cannot honor the space guarantees required by this volume, the volume online operation will fail. It is not advisable to use volumes with their space guarantees disabled. Lack of free space can lead to failure of writes which in turn can appear as data loss to some applications.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver from which the volume is to be brought online. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the name of the volume that is to be brought online.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

### Examples

The following example brings a volume named `vol1` online:

```
cluster::> volume online vol1
Volume 'vs1:vol1' is now online.
```

---

## volume rename

Rename an existing volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume rename` command renames a volume. The volume name must be unique among the other volumes on the same Vserver.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located. For a node's root volume, use the name of the node for this parameter.

**-volume** <volume name> - Volume Name

This specifies the volume that is to be renamed.

**-newname** <volume name> - Volume New Name

This specifies the volume's new name. A volume's name must start with an alphabetic character (a to z or A to Z) and be 203 or fewer characters in length.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

### Examples

The following example renames a volume named `vol3_backup` as `vol3_save` on a Vserver named `vs0`:

```
node::> volume rename -vserver vs0 -volume vol3_backup -newname vol3_save
```

## volume restrict

Restrict an existing volume



---

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume restrict` command puts the volume in restricted state. If the volume is online, then it will be made unavailable for data access as described under `volume offline`.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver from which the volume is to be restricted. If only one data Vserver exists, you do not need to specify this parameter.

**-volume** <volume name> - Volume Name

This specifies the name of the volume that is to be restricted.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). When set to `true`, the command will not return until the operation completes. This parameter applies only to Infinite Volumes. For FlexVol volumes, the command always runs in the foreground.

## Examples

The following example restricts a volume named `vol1`:

```
cluster::> volume restrict voll
Volume 'vsl:voll' is now restricted.
```

## See Also

`volume offline`

---

## volume show-footprint

Display a list of volumes and their data and metadata footprints in their associated aggregate.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume show-footprint` command displays information about the space used in associated aggregates by volumes and features enabled in volumes. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all volumes.

The `volume show-footprint` command is not supported for Infinite Volumes; however, the command displays information about Infinite Volume constituents as if the constituents were FlexVol volumes.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter and the `-volume` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about volumes on the specified Vserver.

[-volume <volume name>] - Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about all volumes matching the specified name.

[-volume-msid <integer>] - Volume MSID

---

If this parameter is specified, the command displays information only about the volume that has the specified MSID.

**[-volume-dsid <integer>]** - Volume DSID

If this parameter is specified, the command displays information only about the volume that has the specified DSID.

**[-vserver-uuid <UUID>]** - Vserver UUID

If this parameter is specified, the command displays information only about the volume on the vservers which has the specified UUID.

**[-aggregate <aggregate name>]** - Aggregate Name

If this parameter is specified, the command displays information only about the volumes that are associated with the specified aggregate.

**[-aggregate-uuid <UUID>]** - Aggregate UUID

If this parameter is specified, the command displays information only about the volumes on the aggregate which have the specified UUID.

**[-hostname <text>]** - Hostname

If this parameter is specified, the command displays information only about the volumes that belong to the specified host.

**[-tape-backup-metafiles-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Tape Backup Metadata Footprint

If this parameter is specified, the command displays information only about the volumes whose tape backup metafiles use the specified amount of space in the aggregate.

**[-tape-backup-metafiles-footprint-percent <percent>]** - Tape Backup Metadata Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose tape backup metafiles use the specified percentage of space in the aggregate.

**[-dedupe-metafiles-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Deduplication Footprint

If this parameter is specified, the command displays information only about the volumes whose deduplication metafiles use the specified amount of space in the aggregate.

**[-dedupe-metafiles-footprint-percent <percent>]** - Deduplication Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose deduplication metafiles use the specified percentage of space in the aggregate.

**[-dedupe-metafiles-temporary-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Temporary Deduplication Footprint

---

If this parameter is specified, the command displays information only about the volumes whose temporary deduplication metafiles use the specified amount of space in the aggregate.

**[-dedupe-metafiles-temporary-footprint-percent <percent>]** - Temporary Deduplication Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose temporary deduplication metafiles use the specified percentage of space in the aggregate.

**[-volume-blocks-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Volume Data Footprint

If this parameter is specified, the command displays information only about the volumes whose data blocks use the specified amount of space in the aggregate.

This field is the total amount of data written to the volume. It includes data in the active file system in the volume as well as data that is consumed by volume Snapshot copies. This row only includes data and not reserved space, so when volumes have reserved files, the volume's total used in the `volume show-space` command output can exceed the value in this row.

**[-volume-blocks-footprint-percent <percent>]** - Volume Data Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose data blocks use the specified percentage of space in the aggregate.

**[-flexvol-metadata-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Flexible Volume Metadata Footprint

If this parameter is specified, the command displays information only about the volumes whose file system metadata uses the specified amount of space in the aggregate.

This field includes the space used or reserved in the aggregate for metadata associated with this volume.

**[-flexvol-metadata-footprint-percent <percent>]** - Flexible Volume Metadata Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose file system metadata uses the specified percentage of space in the aggregate.

**[-delayed-free-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Delayed Free Blocks

If this parameter is specified, the command displays information only about the volumes whose delayed free blocks use the specified amount of space in the aggregate.

When Data ONTAP frees space in a volume, this space is not always immediately shown as free in the aggregate. This is because the operations to free the space in the aggregate are batched for increased performance. Blocks that are declared free

---

in the FlexVol volume but which are not yet free in the aggregate are called "delayed free blocks" until the associated delayed free blocks are processed. For SnapMirror destinations, this row will have a value of 0 and will not be displayed.

**[-delayed-free-footprint-percent <percent>]** - Delayed Free Blocks Percent

If this parameter is specified, the command displays information only about the volumes that have the specified amount of blocks waiting to be freed in the aggregate. This space is called "delayed free blocks".

**[-snapmirror-destination-footprint {<integer>[KB|MB|GB|TB|PB]}]** - SnapMirror Destination Footprint

If this parameter is specified, the command displays information only about the volumes whose SnapMirror transfer uses the specified amount of space in the aggregate.

During a SnapMirror transfer, this row will include incoming SnapMirror data and SnapMirror-triggered delayed free blocks from previous SnapMirror transfers.

**[-snapmirror-destination-footprint-percent <percent>]** - SnapMirror Destination Footprint Percent

If this parameter is specified, the command displays information only about the volumes whose SnapMirror transfer uses the specified percentage of space in the aggregate.

**[-volume-guarantee-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Volume Guarantee

If this parameter is specified, the command displays information only about the volumes whose guarantees use the specified amount of space in the aggregate.

This field includes the amount of space reserved by this volume in the aggregate for future writes. The amount of space reserved depends on the guarantee type (the provisioning mode) of the volume.

For a "volume" guaranteed volume, this is the size of the volume minus the amount in the Volume Data Footprint row.

For a "file" guaranteed volume, this is the sum of all of the space reserved for hole fills and overwrites in all of the space reserved files in the volume.

**[-volume-guarantee-footprint-percent <percent>]** - Volume Guarantee Percent

If this parameter is specified, the command displays information only about the volumes whose guarantees use the specified percentage of space in the aggregate.

**[-total-footprint {<integer>[KB|MB|GB|TB|PB]}]** - Total Footprint

If this parameter is specified, the command displays information only about the volumes which use the specified amount of space in the aggregate. This field is the sum of the other rows in this table.

**[-total-footprint-percent <percent>]** - Total Footprint Percent

If this parameter is specified, the command displays information only about the volumes which use the specified percentage of space in the aggregate.

**[-aggregate-size {<integer>[KB|MB|GB|TB|PB]}]** - Containing Aggregate Size

If this parameter is specified, the command displays information only about the volumes that are associated with an aggregate of the specified size.

## Examples

The following example displays information about all volumes in the system

```
cluster1::> volume show-footprint

Vserver : nodevs
Volume  : vol0

Feature-----
Volume Data Footprint      103.1MB      11%
Volume Guarantee           743.6MB      83%
Flexible Volume Metadata    4.84MB      1%
Delayed Frees               4.82MB      1%
Total Footprint            856.3MB      95%

Vserver : thevs
Volume  : therootvol

Feature-----
Volume Data Footprint      116KB      0%
Volume Guarantee           19.83MB      1%
Flexible Volume Metadata    208KB      0%
Delayed Frees               60KB      0%
Total Footprint            20.20MB      1%

Vserver : thevs
Volume  : thevol

Feature-----
Volume Data Footprint      128KB      0%
Volume Guarantee           2.00GB      76%
Flexible Volume Metadata    11.38MB      0%
Delayed Frees               428KB      0%
Total Footprint            2.01GB      76%

3 entries were displayed.
```

## See Also

volume show-space

---

## volume show-space

Display space usage for volume(s)

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume show-space` command displays information about space usage within the volume. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all volumes.

The `volume show-space` command is not supported for Infinite Volumes; however, the command displays information about Infinite Volume constituents as if the constituents were FlexVol volumes.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter and the `-volume` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about volumes on the specified Vserver.

[-volume <volume name>] - Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about all volumes matching the specified name.

[-volume-msid <integer>] - Volume MSID

---

If this parameter is specified, the command displays information only about the volume that has the specified MSID.

**[-volume-dsid <integer>]** - Volume DSID

If this parameter is specified, the command displays information only about the volume that has the specified DSID.

**[-vserver-uuid <UUID>]** - Vserver UUID

If this parameter is specified, the command displays information only about the volume on the vservers which has the specified UUID.

**[-aggregate <aggregate name>]** - Aggregate Name

If this parameter is specified, the command displays information only about the volumes that are associated with the specified aggregate.

**[-aggregate-uuid <UUID>]** - Aggregate UUID

If this parameter is specified, the command displays information only about the volumes on the aggregate which have the specified UUID.

**[-hostname <text>]** - Hostname

If this parameter is specified, the command displays information only about the volumes that belong to the specified host.

**[-user-data {<integer>[KB|MB|GB|TB|PB]}]** - User Data

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by user data in the volume.

This is the amount of data written to the volume via CIFS, NFS or SAN protocols plus the metadata (for example indirect blocks, directory blocks) directly associated with user files plus the space reserved in the volume for these files (hole and overwrite reserves). This is the same information displayed by running the Unix `du` command on the mount point.

**[-user-data-percent <percent>]** - User Data Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by user data in the volume.

**[-dedupe-metafiles {<integer>[KB|MB|GB|TB|PB]}]** - Deduplication

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by deduplication metafiles in the volume.



---

**[-dedupe-metafiles-percent <percent>]** - Deduplication Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by deduplication metafiles in the volume.

**[-dedupe-metafiles-temporary {<integer>[KB|MB|GB|TB|PB]}]** - Temporary Deduplication

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by temporary deduplication metafiles in the volume.

**[-dedupe-metafiles-temporary-percent <percent>]** - Temporary Deduplication Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by temporary deduplication metafiles in the volume.

**[-filesystem-metadata {<integer>[KB|MB|GB|TB|PB]}]** - Filesystem Metadata

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by file system metadata in the volume.

**[-filesystem-metadata-percent <percent>]** - Filesystem Metadata Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by file system metadata in the volume.

**[-snapmirror-metadata {<integer>[KB|MB|GB|TB|PB]}]** - SnapMirror Metadata

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by SnapMirror metafiles in the volume.

Between SnapMirror transfers, some metadata is maintained to support storage-efficient transfers. During transfers, some additional space is used temporarily. This space is used in all SnapMirror destination volumes.

**[-snapmirror-metadata-percent <percent>]** - SnapMirror Metadata Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by SnapMirror metafiles inside the volume.

**[-tape-backup-metadata {<integer>[KB|MB|GB|TB|PB]}]** - Tape Backup Metadata

---

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by tape backup metafiles in the volume.

**[-tape-backup-metadata-percent <percent>]** - Tape Backup Metadata Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by tape backup metafiles in the volume.

**[-quota-metafiles {<integer>[KB|MB|GB|TB|PB]}]** - Quota Metadata

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by quota metafiles.

**[-quota-metafiles-percent <percent>]** - Quota Metadata Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by quota metafiles.

**[-inodes {<integer>[KB|MB|GB|TB|PB]}]** - Inodes

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by the inode metafile in the volume.

This is the amount of space required to store inodes in the file system and is proportional to the maximum number of files ever created in the volume. The inode file is not compacted or truncated, so if a large number of files are created and then deleted, the inode file does not shrink.

**[-inodes-percent <percent>]** - Inodes Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by the inode metafile in the volume.

**[-snapshot-reserve {<integer>[KB|MB|GB|TB|PB]}]** - Snapshot Reserve

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by the Snapshot reserve in the volume.

**[-snapshot-reserve-percent <percent>]** - Snapshot Reserve Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by the Snapshot reserve in the volume.

**[-snapshot-spill {<integer>[KB|MB|GB|TB|PB]}]** - Snapshot Spill

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by their Snapshot spill.

If Snapshot used space exceeds the Snapshot reserve it is considered to spill out of the reserve. This space cannot be used by the active file system until Snapshots are deleted.

**[-snapshot-spill-percent <percent>] - Snapshot Spill Percent**

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by the Snapshot spill.

**[-total-used {<integer>[KB|MB|GB|TB|PB]] - Total Used**

If this parameter is specified, the command displays information only about the volume or volumes that have the specified amount of space in use by the volume, including the space used by the Snapshot reserve.

This is equivalent to the used field in the output of the `volume show` command.

**[-total-used-percent <percent>] - Total Used Percent**

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space in use by the volume, including the space used by the Snapshot reserve.

## Examples

The following example shows how to display details for all volumes.

```
cluster::>volume show-space
```

```
Vserver : nodevs
Volume  : vol0
```

Feature	Used	Used%
User Data	101.0MB	12%
Filesystem Metadata	100KB	0%
Inodes	1.98MB	0%
Snapshot Reserve	42.57MB	5%
Total Used	145.7MB	17%

```
Vserver : thevs
Volume  : therootvol
```

Feature	Used	Used%
User Data	44KB	0%
Filesystem Metadata	60KB	0%
Inodes	12KB	0%
Snapshot Reserve	1MB	5%
Total Used	1.11MB	6%

```
Vserver : thevs
Volume  : thevol
```

---

Feature	Used	Used%
-----	-----	-----
User Data	40KB	0%
Filesystem Metadata	80KB	0%
Inodes	8KB	0%
Snapshot Reserve	102.4MB	5%
Total Used	102.5MB	5%

3 entries were displayed.

The following example shows all Volumes that have a snap reserve greater than 2 MB:

```
cluster1::> volume show-space -snapshot-reserve >2m
```

```
Vserver : nodevs
Volume  : vol0
```

Feature	Used	Used%
-----	-----	-----
User Data	101.0MB	12%
Filesystem Metadata	100KB	0%
Inodes	1.98MB	0%
Snapshot Reserve	42.57MB	5%
Total Used	145.7MB	17%

```
Vserver : thevs
Volume  : thevol
```

Feature	Used	Used%
-----	-----	-----
User Data	40KB	0%
Filesystem Metadata	80KB	0%
Inodes	8KB	0%
Snapshot Reserve	102.4MB	5%
Total Used	102.5MB	5%

2 entries were displayed.

## See Also

volume show

---

## volume show

Display a list of volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume show` command displays information about volumes. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all volumes:

- Vserver name
- Volume name
- Aggregate name
- State (online, offline, restricted, or force-online)
- Type (RW for read-write, DP for data-protection, or DC for data-cache)
- Size
- Available size
- Percentage of space used

To display detailed information about a single volume, run the command with the `-vserver` and `-volume` parameters. The detailed view provides all of the information in the previous list and the following additional information:

- Name ordinal
- Volume data set ID
- Volume master data set ID
- Volume style (trad, flex or infinitevol)
- Whether the volume is a Cluster volume or Node volume
- Export policy name
- User ID
- Group ID

- 
- Security style (unix, ntfs, mixed or unified)
  - UNIX permissions
  - Junction path
  - Junction path source
  - Whether the junction path is active
  - Parent volume name
  - Vserver root volume
  - Comment
  - Filesystem size
  - Total user-visible size
  - Used size
  - Used percentage
  - Volume nearly full threshold percent
  - Volume full threshold percent
  - Autosize enabled
  - Maximum autosize
  - Autosize increment
  - Minimum autosize
  - Autosize grow threshold percent
  - Autosize shrink threshold percent
  - Autosize mode
  - Total files
  - Files used
  - Maximum directory size
  - Space guarantee style
  - Whether a space guarantee is in effect
  - Whether minimum readahead is enabled
  - Whether access time update is enabled

- 
- Whether Snapshot directory access is enabled
  - Percentage of space reserved for Snapshot copies
  - Percentage of Snapshot copy space used
  - Snapshot policy name
  - Creation time
  - If the filesystem size is fixed
  - Overwrite reserve
  - Fractional reserve
  - Which space management strategy to try first
  - Language
  - Whether there's one data volume per member aggregate
  - Concurrency level
  - Optimization policy
  - Whether the volume is a clone
  - Volume UUID
  - FlexCache cache policy
  - Whether failover is enabled
  - Failover state
  - Extent option
  - Read reallocation option
  - Consistency state
  - Whether volume is quiesced on disk
  - Whether volume is quiesced in memory
  - FlexCache connection status
  - Whether volume contains shared or compressed data
  - Space saved by storage efficiency
  - Percentage of space saved by storage efficiency
  - Space saved by deduplication

- 
- Percentage of space saved by deduplication
  - Space shared by deduplication
  - Space saved by compression
  - Percentage of space saved by compression

To display detailed information about all volumes, run the command with the `-instance` parameter. Fields not supported by Infinite Volumes will display a value of `"_"`.

You can specify additional parameters to display information that matches only those parameters. For example, to display information only about data-protection volumes, run the command with the `-type DP` parameter.

## Parameters

{ **[-fields** <fieldname>, ...]

This specifies the fields that need to be displayed. The fields `Vserver` and `policy` are the default fields (see example).

| **[-junction]**

If this parameter is specified, the command displays the following information:

- Vserver name
- Volume name
- Whether the volume's junction is active
- Junction path
- Junction path source (if the volume is a mirror)

| **[-settings]** (privilege: advanced)

If this parameter is specified, the command displays the following information:

- Vserver name
- Volume name
- Whether minimum readahead is enabled on the volume
- Whether the access time is updated on inodes when a file on the volume is read
- Whether clients have access to `.snapshot` directories



- 
- Whether automatic Snapshot copies are enabled on the volume

| **[-instance ]** }

If this parameter is specified, the command displays information about all entries.

**[-vserver <vserver name>]** - Vserver Name

If this parameter and the `-volume` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about volumes on the specified Vserver.

**[-volume <volume name>]** - Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information about all volumes matching the specified name.

**[-aggregate <aggregate name>]** - Aggregate Name

If this parameter is specified, the command displays information only about the volume or volumes that are located on the specified storage aggregate.

**[-size {<integer>[KB|MB|GB|TB|PB]}]** - Volume Size

If this parameter is specified, the command displays information only about the volume or volumes that have the specified size. Size is the maximum amount of space a volume can consume from its associated aggregate(s), including user data, metadata, Snapshot copies, and Snapshot reserve. Note that for volumes without a `-space-guarantee` of volume, the ability to fill the volume to this maximum size depends on the space available in the associated aggregate or aggregates.

**[-name-ordinal <text>]** - Name Ordinal (privilege: advanced)

If this parameter is specified, it denotes the ordinal assignment used in relation to this volume's name. Ordinals are used to disambiguate volumes that have the same base name on the same controller. A value of "0" indicates that the base volume name is unique on the controller. A value greater than zero indicates that the volume's base name is used by two or more volumes on the same controller, and that appending "(n)" to this volume's name uniquely identifies it on this controller.

**[-dsid <integer>]** - Volume Data Set ID

If this parameter is specified, the command displays information only about the volume or volumes that match the specified data set ID.

**[-msid <integer>]** - Volume Master Data Set ID

If this parameter is specified, the command displays information only about the volume or volumes that match the specified master data set ID.

---

**[-state {online|restricted|offline|force-online|force-offline|mixed}]** - Volume State

If this parameter is specified, the command displays information only about the volume or volumes that have the specified state.

**[-type {RW|DP|DC}]** - Volume Type

If this parameter is specified, the command displays information only about the volume or volumes of the specified volume type (RW for read-write, DP for data-protection, or DC for data-cache).

**[-volume-style {flex|striped|infinitevol}]** - Volume Style

If this parameter is specified, the command displays information only about the volumes that have the specified style. Possible values are flex for FlexVol volumes, and infinitevol for Infinite Volumes.

**[-is-cluster-volume {true|false}]** - Is Cluster-Mode Volume

If this parameter is specified, the command displays information only about volumes that are C-Mode (true) or 7-Mode (false).

**[-is-constituent {true|false}]** - Is Constituent Volume

If this parameter is specified, the command displays information only about volumes that either are or are not constituents of an Infinite Volume, depending on the value provided.

**[-policy <text>]** - Export Policy

If this parameter is specified, the command displays information only about the volume or volumes that use the specified export policy.

**[-user <user name>]** - User ID

If this parameter is specified, the command displays information only about the volume or volumes whose root is owned by the specified user.

**[-group <group name>]** - Group ID

If this parameter is specified, the command displays information only about the volume or volumes whose root is owned by the specified group.

**[-security-style {unix|ntfs|mixed|unified}]** - Security Style

If this parameter is specified, the command displays information only about the volume or volumes that have the specified security style (unix for UNIX mode bits, ntfs for CIFS ACLs, mixed for both styles or unified for Unified UNIX, NFS and CIFS permissions).

**[-unix-permissions <unix perm>]** - UNIX Permissions

If this parameter is specified, the command displays information only about the volume or volumes whose default UNIX permissions match the specified permissions. Specify

---

UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX ls command (for example, -rwxr-x---). For information on UNIX permissions, see the UNIX or Linux documentation.

**[-junction-path <junction path>]** - Junction Path

If this parameter is specified, the command displays information only about the volume or volumes that have the specified junction path.

**[-junction-path-source {RW volume|LS mirror}]** - Junction Path Source

If this parameter is specified, the command displays information only about the volume or volumes that have the specified junction path source.

**[-junction-active {true|false}]** - Junction Active (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes whose junction paths have the specified status.

**[-junction-parent <volume name>]** - Junction Parent Volume

If this parameter is specified, the command displays information only about the volume or volumes that have the specified parent volume.

**[-vsroot {true|false}]** - Vserver Root Volume (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified setting; that is, whether they are the root volumes for their Vservers.

**[-comment <text>]** - Comment

If this parameter is specified, the command displays information only about the volume or volumes that match the specified comment text.

**[-available <integer>[KB|MB|GB|TB|PB]]** - Available Size

If this parameter is specified, the command displays information only about the volume or volumes that have the specified available size. Available is the amount of free space currently available to be used by this volume. For a volume with a `-space-guarantee` of type `volume`, available is always `-total` minus `-used`. For volumes that do not have a `-space-guarantee` of type `volume`, available could be reduced if the volume's associated aggregate or aggregates are space constrained.

**[-filesystem-size <integer>[KB|MB|GB|TB|PB]]** - Filesystem Size

If this parameter is specified, the command displays information only about the volume or volumes that have the specified filesystem size. Filesystem size is the same as the volume's `-size` unless the volume is or was a physical replica destination. In this case, the file system size corresponds to the `-size` of the source volume, until `-filesystem-size-fixed` is set to `false`.

---

**[-total {<integer>[KB|MB|GB|TB|PB]}}** - Total User-Visible Size

If this parameter is specified, the command displays information only about the volume or volumes that have the specified total size. Total is the total space available for user data and file system metadata. It does not include the Snapshot reserve.

**[-used {<integer>[KB|MB|GB|TB|PB]}}** - Used Size

If this parameter is specified, the command displays information only about the volume or volumes that have the specified used size. Used is the amount of space occupied by user data and file system metadata. It includes Snapshot spill (the amount of space by which Snapshot copies exceed Snapshot reserve). It does not include the Snapshot reserve.

**[-percent-used <percent>]** - Used Percentage

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of used space. This row is based on a value of used space that includes the space used by Snapshot copies or the Snapshot reserve (whichever is greater) in relation to the current volume size.

**[-space-nearly-full-threshold-percent <percent>]** - Volume Nearly Full Threshold Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified nearly full threshold percent.

**[-space-full-threshold-percent <percent>]** - Volume Full Threshold Percent

If this parameter is specified, the command displays information only about the volume or volumes that have the specified full threshold percent.

**[-max-autosize {<integer>[KB|MB|GB|TB|PB]}}** - Maximum Autosize (for flexvols only)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified maximum automatic size.

**[-autosize-increment | -i {<integer>[KB|MB|GB|TB|PB]}}** - Autosize Increment (for flexvols only)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified increment size for automatic sizing.

**[-min-autosize {<integer>[KB|MB|GB|TB|PB]}}** - Minimum Autosize

If this parameter is specified, the command displays information only about the volume or volumes that have the specified minimum automatic size.

**[-autosize-grow-threshold-percent <percent>]** - Autosize Grow Threshold Percentage

---

If this parameter is specified, the command displays information only about the volume or volumes that have the specified automatic grow used space threshold percentage.

**[-autosize-shrink-threshold-percent <percent>]** - Autosize Shrink Threshold Percentage

If this parameter is specified, the command displays information only about the volume or volumes that have the specified automatic shrink used space threshold percentage.

**[-autosize-mode {off|grow|grow\_shrink}]** - Autosize Mode

If this parameter is specified, the command displays information only about the volume or volumes that have the specified automatic sizing mode setting.

**[-autosize {true|false}]** - Autosize Enabled (for flexvols only)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified automatic sizing setting.

**[-files <integer>]** - Total Files (for user-visible data)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified number of files.

**[-files-used <integer>]** - Files Used (for user-visible data)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified number of files used.

**[-maxdir-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Directory Size (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified maximum directory size.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

If this parameter is specified, the command displays information only about the volume or volumes that have the specified space-reservation policy. If the value of `-space-guarantee` is `none`, the value of `-space-guarantee-enabled` is always `true`. In other words, because there is no guarantee, the guarantee is always in effect. If the value of `-space-guarantee` is `volume`, the value of `-space-guarantee-enabled` can be `true` or `false`, depending on whether the guaranteed amount of space was available when the volume was mounted.

**[-space-guarantee-enabled {true|false}]** - Space Guarantee in Effect

If this parameter is specified, the command displays information only about the volume or volumes that have the specified space-guarantee setting. If the value of `-space-guarantee` is `none`, the value of `-space-guarantee-enabled` is always `true`. In other words, because there is no guarantee, the guarantee is always in effect. If the

---

value of `-space-guarantee` is volume, the value of `-space-guarantee-enabled` can be true or false, depending on whether the guaranteed amount of space was available when the volume was mounted.

**`[-min-readahead {true|false}]`** - Minimum Read Ahead (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified minimum-readahead setting.

**`[-atime-update {true|false}]`** - Access Time Update Enabled (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that have the specified access-time update setting.

**`[-snapdir-access {true|false}]`** - Snapshot Directory Access Enabled

If this parameter is specified, the command displays information only about the volume or volumes that have the specified Snapshot-copy access setting.

**`[-percent-snapshot-space <percent>]`** - Space Reserved for Snapshots

If this parameter is specified, the command displays information only about the volume or volumes that have the specified percentage of space reserved for Snapshot copies.

**`[-snapshot-space-used <percent_no_limit>]`** - Snapshot Reserve Used

If this parameter is specified, the command displays information only about the volume or volumes that have the specified used percentage of the reserve for Snapshot copies.

**`[-snapshot-policy <snapshot policy>]`** - Snapshot Policy

If this parameter is specified, the command displays information only about the volume or volumes that use the specified Snapshot policy.

**`[-create-time <Date>]`** - Creation Time

If this parameter is specified, the command displays information only about the volume or volumes that have the specified creation time.

**`[-language <Language code>]`** - Language

If this parameter is specified, the command displays information only about the volume or volumes that store data in the specified language. To determine the available languages, enter `volume show-language?` at the clustershell command prompt.

**`[-clone-volume {true|false}]`** - Clone Volume

If this parameter is specified, the command displays information only about volumes that are clones (true) or not clones (false).

**`[-antivirus-on-access-policy <antivirus policy>]`** - Antivirus On-Access Policy

---

If this parameter is specified, the command displays information only about volumes that have the specified antivirus on-access policy. For more information on the antivirus on-access policies see the `antivirus on-access policy show` command.

**[-flexcache-cache-policy <cache policy>]** - FlexCache Cache Policy (privilege: advanced)

If this parameter is specified, the command displays information only about volumes that match the specified flexcache cache-policy.

**[-flexcache-min-reserve <{integer}>[KB|MB|GB|TB|PB]]** - FlexCache Minimum Reserve (privilege: advanced)

If this parameter is specified, the command displays information only about member volumes that match the specified FlexCache minimum reserve.

**[-node <{nodename}>|local]** - Node name

If this parameter is specified, the command displays information only the volume or volumes that are located on the specified storage system.

**[-uuid <UUID>]** - UUID of the Volume (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified UUID.

**[-nvfail {on|off}]** - NVFAIL Option

If this parameter is specified, the command displays information only about volumes for which failover is enabled (on) or disabled (off).

**[-in-nvfailed-state {true|false}]** - Volume's Nvfailed State (privilege: advanced)

If this parameter is specified, the command displays information only about volumes which are in the failed over state (true) or not (false).

**[-filesystems-size-fixed {true|false}]** - Is File System Size Fixed

If this parameter is specified, the command displays information only about the volume or volumes that have the specified `filesystems-size-fixed` setting.

**[-extent-enabled {off|on|space-optimized}]** - Extent Option

If this parameter is specified, the command displays information only about volumes that have extents enabled (on), not enabled (off) or space optimized (space-optimized).

**[-overwrite-reserve <{integer}>[KB|MB|GB|TB|PB]]** - Reserved Space for Overwrites

If this parameter is specified, the command displays information only about the volume or volumes that have the specified `overwrite-reserve` setting.

**[-fractional-reserve <percent>]** - Fractional Reserve

---

If this parameter is specified, the command displays information only about the volume or volumes that have the specified `fractional-reserve` setting.

**[-snapshot-clone-dependency {on|off}]** - Snapshot Cloning Dependency

If this parameter is specified, the command displays information only about the volume or volumes that have the specified `snapshot-clone-dependency` value.

**[-space-mgmt-try-first {volume\_grow|snap\_delete}]** - Primary Space Management Strategy

If this parameter is specified, the command displays information only about the volume or volumes that have the specified `space-mgmt-try-first` setting. Possible values are `volume_grow` and `snap_delete`.

**[-read-realloc {off|on|space-optimized}]** - Read Reallocation Option

If this parameter is specified, the command displays information only about volumes that have read reallocation enabled (on), not enabled (off) or space optimized (space-optimized).

**[-is-inconsistent {true|false}]** - Inconsistency in the File System

If this parameter is specified, the command displays information only about volumes that are inconsistent (true) or consistent (false) in the file system.

**[-is-quieted-on-disk {true|false}]** - Is Volume Quiesced (On-Disk)

If this parameter is specified, the command displays information only about volumes that are quiesced (true) or not quiesced (false) on disk.

**[-is-quieted-in-memory {true|false}]** - Is Volume Quiesced (In-Memory)

If this parameter is specified, the command displays information only about volumes that are quiesced (true) or not quiesced (false) in memory.

**[-transition-state <state>]** - Transition Operation State (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified transition state.

**[-transition-behavior {data-move|data-protection|none}]** - Transition Behavior (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified transition behavior. Possible values are:

- `data-move`: Volumes that are being moved from a system operating in 7-Mode.
- `data-protection`: Volumes that are being replicated from a system operating in 7-Mode for disaster recovery.



- 
- none: Volumes that are not part of transition.

**[-is-copied-for-transition {true|false}]** - Copied for Transition (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified value based on whether the volume is copied for transition or not.

**[-is-transitioned {true|false}]** - Transitioned (privilege: advanced)

If this parameter is specified, the command displays information only about the volume or volumes that match the specified value based on whether the volume is transitioned or not.

**[-is-sis-volume {true|false}]** - Volume Contains Shared or Compressed Data

If this parameter is specified, the command displays information only about those volumes that match the specified storage efficiency setting. Infinite Volumes will report the aggregated setting of their constituent data volumes as true or false if all constituents have the same setting, otherwise no value will be reported.

**[-sis-space-saved {<integer>[KB|MB|GB|TB|PB]}]** - Space Saved by Storage Efficiency

If this parameter is specified, the command displays information only about those volumes that have the specified amount of space saved by the storage efficiency technology.

**[-sis-space-saved-percent <percent>]** - Percentage Saved by Storage Efficiency

If this parameter is specified, the command displays information only about those volumes that have the specified percentage of space saved by the storage efficiency technology.

**[-dedupe-space-saved {<integer>[KB|MB|GB|TB|PB]}]** - Space Saved by Deduplication

If this parameter is specified, the command displays information only about those volumes that have the specified amount of space saved due to deduplication.

**[-dedupe-space-saved-percent <percent>]** - Percentage Saved by Deduplication

If this parameter is specified, the command displays information only about those volumes that have the specified percentage of space saved due to deduplication.

**[-dedupe-space-shared {<integer>[KB|MB|GB|TB|PB]}]** - Space Shared by Deduplication

If this parameter is specified, the command displays information only about those volumes that have the specified amount of shared space due to deduplication.

---

**[-compression-space-saved {<integer>[KB|MB|GB|TB|PB]}]** - Space Saved by Compression

If this parameter is specified, the command displays information only about those volumes that have the specified amount of space saved due to compression.

**[-compression-space-saved-percent <percent>]** - Percentage Space Saved by Compression

If this parameter is specified, the command displays information only about those volumes that have the specified percentage of space saved due to compression.

**[-block-type {32-bit|64-bit}]** - Block Type

If this parameter is specified, the command displays information about only the volumes with the specified indirect block format. Possible values are 32-bit to display 32-bit volumes and 64-bit to display 64-bit volumes.

**[-flexcache-connection-status <text>]** - FlexCache Connection Status

If this parameter is specified, the command displays information only about volumes that match the specified FlexCache connection status.

**[-is-moving {true|false}]** - Is Volume Moving

If this parameter is specified, the command displays information only about volumes that are moving (true) or not moving (false).

**[-hybrid-cache-eligibility {read|read-write}]** - Flash Pool Caching Eligibility

If this parameter is specified, the command displays information only about the volume or volumes with the specified Flash Pool caching attributes. Possible caching attributes are:

- 'read' ... Indicates that the volume cannot participate in write caching.
- 'read-write' ... Indicates that the volume can participate in read and write caching.

**[-hybrid-cache-write-caching-ineligibility-reason <text>]** - Flash Pool Write Caching Ineligibility Reason

If this parameter is specified, the command displays information only about the volume or volumes which are ineligible to participate in write caching due to the specified reason.

**[-enable-snapdiff {true|false}]** - Create Namespace Mirror Constituents For SnapDiff Use

---

Setting this parameter displays information only about Infinite Volumes that either do or do not have namespace mirror constituents for SnapDiff use, depending on the value provided. This parameter applies to Infinite Volumes only.

**[-unreachable-attr-action {return-generated|wait}]** - Action When Attributes Are Not Reachable (privilege: advanced)

This parameter specifies the information that an Infinite Volume returns when a client lists a directory that contains one or more files with inaccessible attributes. If this parameter is specified, the command displays information only about volumes that match the specified action. This parameter is not supported for FlexVol volumes.

**[-max-namespace-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Namespace Constituent (privilege: advanced)

If this parameter is specified, the command displays information only about volumes that match the specified namespace constituent size.

**[-max-data-constituent-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of Each Data Constituent (privilege: advanced)

If this parameter is specified, the command displays information only about the Infinite Volume or Infinite Volumes that have the specified maximum data constituent size. This parameter applies to Infinite Volumes only.

**[-qos-policy-group <text>]** - QoS Policy Group Name

If this parameter is specified, the command displays information only about volumes that match the specified Qos policy group.

**[-is-volume-in-cutover {true|false}]** - Is Volume Move in Cutover Phase

If this parameter is specified, the command displays information only about volumes that are in the cutover phase (true) or not in the cutover phase (false) of a volume move.

**[-snapshot-count <integer>]** - Number of Snapshot Copies in the Volume

If this parameter is specified, the command displays information only about the volumes that have the specified number of Snapshot copies.

## Examples

The following example displays information about all volumes on the Vserver named vs1:

```
cluster::> volume show -vserver vs1
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
vs1	vol1	aggr1	online	RW	2GB	1.9GB	5%
vs1	vol1_dr	aggr0_dp	online	DP	200GB	160.0GB	20%
vs1	vol2	aggr0	online	RW	150GB	110.3GB	26%
vs1	vol2_dr	aggr0_dp	online	DP	150GB	110.3GB	26%
vs1	vol3	aggr1	online	RW	150GB	120.0GB	20%

vs1	vol3_dr	aggr1_dp	online	DP	150GB	120.0GB	20%
vs1	vol4	aggr1	online	RW	200GB	159.8GB	20%
vs1	vol4_dr	aggr1_dp	online	DP	200GB	159.8GB	20%
vs1	vol5	aggr2	online	RW	200GB	102.3GB	48%
vs1	vol5_dr	aggr2_dp	online	DP	200GB	102.3GB	48%
vs1	vol6	aggr2	online	RW	150GB	117.2GB	21%
vs1	vol6_dr	aggr2_dp	online	DP	150GB	117.2GB	21%
vs1	vol7	aggr3	online	RW	150GB	118.5GB	20%
vs1	vol7_dr	aggr3_dp	online	DP	150GB	118.5GB	20%
vs1	vol8	aggr3	online	RW	150GB	90.03GB	39%
vs1	vol8_dr	aggr3_dp	online	DP	150GB	90.03GB	39%
vs1	vol9	aggr4	online	RW	150GB	43.67GB	70%
vs1	vol9_dr	aggr4_dp	online	DP	150GB	43.67GB	70%
vs1	vol10	aggr4	online	RW	150GB	108.7GB	27%
vs1	vol10_dr	aggr4_dp	online	DP	150GB	108.7GB	27%
vs1	vol11	aggr5	online	RW	250GB	45.65GB	81%
vs1	vol11_dr	aggr5_dp	online	DP	250GB	45.65GB	81%

22 entries were displayed.

The following example displays detailed information about a volume named vol1 on a Vserver named vs1:

```
cluster::*> volume show -vserver vs1 -volume vol1
```

```

Vserver Name: vs1
Volume Name: vol1
Aggregate Name: aggr1
Volume Size: 2GB
Volume Data Set ID: 1026
Volume Master Data Set ID: 2147484674
Volume State: online
Volume Type: RW
Volume Style: flex
Is Cluster-Mode Volume: true
Export Policy: default
User ID: root
Group ID: daemon
Security Style: mixed
Unix Permissions: ---rwx-----
Junction Path: -
Junction Path Source: -
Junction Active: -
Parent Volume: -
Comment:
Available Size: 1.90GB
Filesystem Size: 2GB
Total User-Visible Size: 1.90GB
Used Size: 192KB
Used Percentage: 5%
Volume Nearly Full Threshold Percent: 90%
Volume Full Threshold Percent: 99%
Autosize Enabled (for flexvols only): false
Maximum Autosize (for flexvols only): 2.40GB
Autosize Increment (for flexvols only): 102.4MB
Minimum Autosize: 1.9GB
Autosize Grow Threshold Percentage: 85%
Autosize Shrink Threshold Percentage: 35%
Autosize Mode: grow_shrink
Total Files (For User-Visible Data): 62244
Files Used (For User-Visible Data): 96
Space Guarantee Style: volume
Space Guarantee In Effect: true
Space Reserved For Snapshots: 5%
Snapshot Reserve Used: 0%
Snapshot Policy: none
Creation Time: Sat Jan 22 01:45:41 2011
Clone Volume: false
Antivirus On-Access Policy: default
NVFAIL option: off
Is File System Size Fixed: false
Extent Option: off
Reserved Space for Overwrites: 0.00B
Fractional Reserve: 100%
Automatic snapshots: false
Snapshot Cloning Dependency: off
Primary Space Management Strategy: volume_grow
Read Reallocation Option: off
Naming Scheme for sched snapshots: create_time
Inconsistency In The File System: false

```

---

```
Is Volume Quiesced (On-Disk): false
Is Volume Quiesced (In-Memory): false
Transition Operation State: none
Copied for Transition: false
Transitioned: true
Volume Contains Shared or Compressed Data: false
Space Saved by Storage Efficiency: 0.00B
Percentage Saved by Storage Efficiency: 0%
Space Saved by Deduplication: 0.00B
Percentage Saved by Deduplication: 0%
Space Shared by Deduplication: 0.00B
Space Saved by Compression: 0.00B
Percentage Space Saved by Compression: 0%
Block Type: 32-bit
FlexCache Connection Status: -
Constituent Volume Role: -
Is Volume Moving: false
Is Volume Move in Cutover Phase: false
Hybrid Cache Eligibility: read-write
Hybrid Cache Write Caching Ineligibility Reason: -
Number of Snapshot Copies in the Volume: 0
```

## See Also

antivirus on-access policy show

---

## volume size

Set/Display the size of the volume.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume size` command allows the user to set or display the volume size. If new-size is not specified then the current volume size is displayed.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter can be used to specify the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This parameter specifies the volume for which the user wants to set or display the size.

**[-new-size <text>] - [+|-]<New Size>**

This optional parameter specifies the size of the volume. It can be used to set the volume size to a particular number or grow/shrink the size by a particular amount. The size is specified as a number (preceded with a sign for relative growth/shrinkage) followed by a unit designation: k (kilobytes), m (megabytes), g (gigabytes), or t (terabytes). If the unit designation is not specified, bytes are used as the unit, and the specified number is rounded up to the nearest 4 KB. The minimum size for a flexible volume is 20 MB, and the maximum size depends on hardware platform and free space in the containing aggregate. If the volume's space guarantee is currently disabled, its size cannot be increased. This parameter is not supported on Infinite Volumes that are managed by storage services.

### Examples

The following example shows the size of a volume called vol1.

```
cluster::> vol size vol1
(volume size)
vol size: Flexible volume 'vsl:vol1' has size 2g.
```

The following example sets the size of a volume called vol1 to 1GB.

```
cluster::> vol size vol1 1g
(volume size)
vol size: Flexible volume 'vsl:vol1' size set to 1g.
```

The following example increases the size of a volume called vol1 by 500MB.

---

```
cluster::> vol size vol1 +500m
(volume size)
vol size: Flexible volume 'vs1:vol1' size set to 1.49g.
```

The following example decreases the size of a volume called vol1 by 250MB.

```
cluster::> vol size vol1 -250m
(volume size)
vol size: Flexible volume 'vs1:vol1' size set to 1.24g.
```

## volume unmount

Unmount a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume unmount` command unmounts a volume from its parent volume. The volume can be remounted at the same or a different location by using the `volume mount` command.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the volume that is to be unmounted.

### Examples

The following example unmounts a volume named vol2 on a Vserver named vs0:

```
node::> volume unmount -vserver vs0 -volume vol2
```

### See Also

`volume mount`

---

## volume clone create

Create a FlexClone volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone create` command creates a FlexClone volume on the aggregate containing the specified parent volume. This command is not supported on Infinite Volumes. You can optionally specify the following attributes for the new FlexClone volume:

- Vserver on which the parent volume resides
- Name of the FlexClone parent snapshot
- Junction path where FlexClone volume should be mounted
- State of the junction path
- Space guarantee style (none, volume or file)
- Comment
- Whether the `volume clone create` command runs as a foreground or background process

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the parent volume resides. If only one data Vserver exists, you do not need to specify this parameter.

**-flexclone** <volume name> - FlexClone Volume

This specifies the name of the FlexClone volume. The name must be unique within the hosting Vserver.

**[-type {RW|DP}]** - FlexClone Type

This parameter specifies the type of FlexClone volume. A read-only FlexClone volume is created if you specify the type as DP; otherwise a read-write FlexClone volume is created.

**-parent-volume | -b** <volume name> - FlexClone Parent Volume



---

This specifies the name of parent volume from which the FlexClone clone volume is derived.

**[-parent-snapshot <snapshot name>]** - FlexClone Parent Snapshot

This specifies the name of the parent snapshot from which the FlexClone clone volume is derived.

**[-junction-path <junction path>]** - Junction Path

This specifies the junction path at which the new FlexClone clone volume should be mounted.

**[-junction-active {true|false}]** - Junction Active

This optionally specifies whether the volume's junction path is active. The default setting is `true`. If the junction path is inactive, the volume does not appear in the Vserver's namespace. This parameter is available only at the advanced privilege level and higher.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

This optionally specifies the space-reservation policy for the FlexClone volume. A value of `file` reserves space only for space-reserved files within the FlexClone volume. A value of `volume` reserves space on the aggregate for the entire volume. A value of `none` reserves no space on the aggregate, meaning that writes can fail if the aggregate runs out of space. The default setting is inherited from the parent volume.

**[-comment <text>]** - Comment

This optionally specifies a comment for the FlexClone volume.

**[-foreground {true|false}]** - Foreground Process

This optionally specifies whether the FlexClone volume create operation runs as a foreground process. The default setting is `true` (that is, the operation runs in the foreground).

**[-qos-policy-group <text>]** - QoS Policy Group Name

This parameter optionally specifies which QoS policy group to apply to the FlexClone volume. The policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to the FlexClone volume, the system does not monitor and control the traffic to the volume.

## Examples

The following command creates a FlexClone volume `fc_vol_1` from parent volume `fv2` on Vserver `vs1` and the job runs as a foreground process.

---

```
cluster1::> volume clone create -vserver vs1 -flexclone fc_vol_1 -parent-  
volume fv2 -junction-active true -foreground true -comment "Testing FlexClone  
creation"  
cluster1::> volume clone show fc_vol_1 -vserver vs1  
      Vserver Name: vs1  
      FlexClone Volume: fc_vol_1  
      FlexClone Parent Volume: fv2  
      FlexClone Parent Snapshot: clone_fc_vol_1.0  
      Junction Path: -  
      Junction Active: -  
      Space Guarantee Style: volume  
      Space Guarantee In Effect: true  
      FlexClone Aggregate: test_aggr  
      FlexClone Data Set ID: 1046  
FlexClone Master Data Set ID: 2147484694  
      FlexClone Size: 19MB  
      Used Size: 108KB  
      Split Estimate: 0.00B  
      Inodes processed: -  
      Total Inodes: -  
      Percentage complete: -  
      Blocks Scanned: -  
      Blocks Updated: -  
      Comment: Testing FlexClone creation
```

---

## volume clone show

Display a list of FlexClones

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone show` command displays information about FlexClone clone volumes. This command is not supported on Infinite Volumes. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays the following information about all FlexClone volume clones:

- Vserver name
- FlexClone volume name
- Parent volume name
- Parent snapshot name
- Whether a FlexClone volume is online or offline

To obtain detailed information about a single FlexClone volume, run the command with the `-vserver` and `-flexclone` parameters. The detailed view provides all of the information in the previous list and the following additional information:

- Junction path
- Whether the junction path is active
- Space guarantee style
- Whether a space guarantee is in effect
- Aggregate containing the FlexClone volume
- Data Set ID of FlexClone volume
- Master Data Set ID of FlexClone volume
- Total size of FlexClone volume
- Used Size of Flexclone volume
- Estimate of free disk space required to split FlexClone volume from parent volume
- Number of Inodes processed during clone splitting

- Total Inodes to be processed during clone splitting
- Percentage of Inode processing complete
- Total number of Blocks scanned for clone splitting
- Total number of Blocks updated for clone splitting
- QoS policy group assigned to the FlexClone volume

To display detailed information about all FlexClone volumes, run the command with the `-instance` parameter.

You can specify additional parameters to display information that matches only those parameters.

## Parameters

{ **[-fields <fieldname>, ...]**

If this parameter is specified, the command displays information about the specified fields only, for the FlexClone volumes.

| **[-estimate ]**

If this parameter is specified, the command displays an estimate of the free disk space required in the aggregate to split the indicated clone volume from its underlying parent volume. The value reported may differ from the space actually required to perform the split, especially if the clone volume is changing when the split is being performed.

| **[-instance ] }**

If this parameter is specified, the command displays detailed information about FlexClone volumes. If the `-flexclone` option is also specified, the command displays detailed information about one FlexClone volume.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays summary information of all FlexClone volumes residing on the specified Vserver. If `-flexclone` is also specified, the command displays detailed information about the specified FlexClone volume.

**[-flexclone <volume name>]** - FlexClone Volume

If this parameter is specified, the command displays summary information of the specified FlexClone volume. If `-vserver` option is also specified, the command displays detailed information about the FlexClone volume.

**[-type {RW|DP}]** - FlexClone Type

---

This parameter specifies the type of FlexClone volume. A read-only FlexClone volume is created if you specify the type as DP; otherwise a read-write FlexClone volume is created.

**[-parent-volume | -b <volume name>]** - FlexClone Parent Volume

If this parameter is specified, the command displays summary information of all the FlexClone volumes that are clones of this parent volume.

**[-parent-snapshot <snapshot name>]** - FlexClone Parent Snapshot

If this parameter is specified, the command displays summary information of all the FlexClone volumes that are clones of the parent volume to which this snapshot belongs.

**[-state {online|restricted|offline|force-online|force-offline|mixed}]** - FlexClone Volume State

If this parameter is specified, the command displays summary information of all the FlexClone volumes that have the specified state.

**[-junction-path <junction path>]** - Junction Path

If this parameter is specified, the command displays information only about the volume or volumes that have the specified junction path.

**[-junction-active {true|false}]** - Junction Active

If this parameter is specified, the command displays information only about the volume or volumes whose junction paths have the specified status.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

If this parameter is specified, the command displays information only about the volumes that have the specified space-reservation policy.

**[-space-guarantee-enabled {true|false}]** - Space Guarantee In Effect

If this parameter is specified, the command displays information only about the volumes that have the specified space-guarantee setting.

**[-aggregate <aggregate name>]** - FlexClone Aggregate

If this parameter is specified, the command displays information about all the FlexClone volumes that reside on the specified storage aggregate.

**[-dsid <integer>]** - FlexClone Data Set ID

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified Data Set ID.

**[-msid <integer>]** - FlexClone Master Data Set ID

---

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified Master Data Set ID.

**[-size {<integer>[KB|MB|GB|TB|PB]}]** - FlexClone Size

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified size.

**[-used {<integer>[KB|MB|GB|TB|PB]}]** - Used Size

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified amount of used space.

**[-split-estimate {<integer>[KB|MB|GB|TB|PB]}]** - Split Estimate

If this parameter is specified, the command displays information about all the FlexClone volumes that require the specified amount of free disk space for splitting from the parent.

**[-inodes-processed <integer>]** - Inodes Processed

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified number of Inodes processed for splitting the FlexClone volume from its parent volume.

**[-inodes-total <integer>]** - Total Inodes

If this parameter is specified, the command displays information about all the FlexClone volumes that have the specified number of total Inodes.

**[-inode-percentage-complete <integer>]** - Percentage Complete

If this parameter is specified, the command displays information about all the FlexClone volumes that have specified percentage of Inodes processed for splitting the FlexClone volume from its parent volume.

**[-blocks-scanned <integer>]** - Blocks Scanned

If this parameter is specified, the command displays information about all FlexClone volumes that have specified number of blocks scanned for splitting the FlexClone volume from its parent volume.

**[-blocks-updated <integer>]** - Blocks Updated

If this parameter is specified, the command displays information about all FlexClone volumes that have specified number of blocks updated for after splitting the FlexClone volume from its parent volume.

**[-comment <text>]** - Comment

---

If this parameter is specified, the command displays information for all the FlexClone volumes that have the specified comment.

**[-qos-policy-group <text>]** - QoS Policy Group Name

If this parameter is specified, the command displays information for all the FlexClone volumes that have the specified QoS policy group.

## Examples

The following example displays detailed information about all FlexClone volumes on Vserver vs0:

```
cluster1::> volume clone show -vserver vs0
(volume clone show)
Vserver  FlexClone      Parent-Volume  Parent-Snapshot
-----  -
vs0      fc_vol_1          test_vol      clone_fc_vol_1.0
         fc_vol_2          test_vol2     clone_fc_vol_2.0
         fc_vol_3          tv9           clone_fc_vol_3.0
         tv8             tv7           clone_tv8.0
         tv9             test_vol2     clone_tv9.0
5 entries were displayed.
```

The following example displays detailed information about FlexClone volume fc\_vol\_2 on Vserver vs0:

```
cluster1::> volume clone show -vserver vs0 -flexclone fc_vol_2
Vserver Name: vs0
FlexClone Volume: fc_vol_2
FlexClone Parent Volume: test_vol2
FlexClone Parent Snapshot: clone_fc_vol_2.0
Junction Path: -
Junction Active: -
Space Guarantee Style: volume
Space Guarantee In Effect: true
FlexClone Aggregate: test_aggr
FlexClone Data Set ID: 1038
FlexClone Master Data Set ID: 2147484686
FlexClone Size: 47.50MB
Used Size: 128KB
Split Estimate: 0.00B
Inodes processed: -
Total Inodes: -
Percentage complete: -
Blocks Scanned: -
Blocks Updated: -
Comment:
Qos Policy Group Name: pg1
```

The following example displays summary information about all FlexClone volumes residing on Vserver vs0 along with the fields msid, dsid, state and parent-volume.

```
cluster1::> volume clone show -vserver vs0 -fields msid, dsid, state, parent-
volume
vserver flexclone parent-volume state dsid msid
-----  -
vs0      fc_vol_1      test_vol      online 1037 2147484685
vs0      fc_vol_3      tv9          online 1039 2147484687
vs0      flex_clone1
vs0      fc_vol_1      online 1041 2147484689
vs0      fv_2          fc_vol_1      online 1043 2147484691
vs0      tv9          test_vol2     online 1036 2147484684
```

---

5 entries were displayed.

The following example displays summary information about all FlexClone volumes residing on Vserver `vs0` along with `space-guarantee-enabled` and `space-guarantee` information about each FlexClone volume.

```
cluster1::> vol clone show -vserver vs0 -fields space-guarantee-enabled, space-
guarantee
(volume clone show)
vserver flexclone space-guarantee space-guarantee-enabled
-----
vs0      fc_vol_1  volume      true
vs0      fc_vol_3  volume      true
vs0      flex_clone1
vs0      volume
vs0      fv_2      volume      true
vs0      tv9       volume      true
5 entries were displayed.
```



---

## volume clone split estimate

Estimates the space required by the containing-aggregate to split the FlexClone volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone split estimate` command displays an estimate of the free disk space required in the aggregate to split the indicated clone volume from its underlying parent volume. The value reported might differ from the space actually required to perform the split, especially if the clone volume is changing when the split is being performed. This command is not supported on Infinite Volumes.

### Parameters

**[-vserver <vserver name>]** - Vserver Name

This specifies the estimates for free disk space required for splitting FlexClone volumes residing on this Vserver. If the `-flexclone` option is also specified, then the command displays the free disk space estimate only for the specified FlexClone volume residing on the specified Vserver.

**[-flexclone <volume name>]** - FlexClone Volume

This specifies the free disk space estimate for splitting this FlexClone volume.

**[-type {RW|DP}]** - FlexClone Type

This parameter specifies the type of FlexClone volume. A read-only FlexClone volume is created if you specify the type as DP; otherwise a read-write FlexClone volume is created.

**[-parent-volume | -b <volume name>]** - FlexClone Parent Volume

This specifies the free disk space estimates for splitting the FlexClone volumes cloned off this parent volume.

**[-parent-snapshot <snapshot name>]** - FlexClone Parent Snapshot

This specifies the free disk space estimates for splitting the FlexClone volumes cloned off this parent snapshot.

**[-state {online|restricted|offline|force-online|force-offline|mixed}]** - FlexClone Volume State

---

This specifies the free disk space estimates for splitting the FlexClone volumes with the specified state.

**[-junction-path <junction path>]** - Junction Path

This specifies the free disk space estimates for splitting the FlexClone volumes mounted at this junction path.

**[-junction-active {true|false}]** - Junction Active

If this specified, the command displays the free disk space estimate for splitting the FlexClone volumes with the specified junction path status.

**[-space-guarantee | -s {none|volume|file}]** - Space Guarantee Style

This specifies the free disk space estimates for splitting the FlexClone volumes with the specified type of space guarantee.

**[-space-guarantee-enabled {true|false}]** - Space Guarantee In Effect

This specifies the free disk space estimates for splitting the FlexClone volumes with the specified state of space guarantee.

**[-aggregate <aggregate name>]** - FlexClone Aggregate

This specifies the free disk space estimates for splitting the FlexClone volumes residing on the specified aggregate.

**[-dsid <integer>]** - FlexClone Data Set ID

This specifies the free disk space estimates for splitting the FlexClone volume with the specified DSID (data set ID).

**[-msid <integer>]** - FlexClone Master Data Set ID

This specifies the free disk space estimates for splitting the FlexClone volumes with the specified MSID (master data set ID).

**[-size {<integer>[KB|MB|GB|TB|PB]}]** - FlexClone Size

This specifies the free disk space estimates for splitting FlexClone volumes with the specified size.

**[-used {<integer>[KB|MB|GB|TB|PB]}]** - Used Size

This specifies the free disk space estimates for splitting the FlexClone volumes with the specified amount of used disk space.

**[-split-estimate {<integer>[KB|MB|GB|TB|PB]}]** - Split Estimate

This specifies the free disk space estimates for splitting the FlexClone volumes which match with the specified free disk space estimate for splitting.

---

**[-inodes-processed <integer>]** - Inodes Processed

This specifies the free disk space estimates for splitting the FlexClone volumes for which the specified number of Inodes have been processed already.

**[-inodes-total <integer>]** - Total Inodes

This specifies the free disk space estimates for splitting the FlexClone volumes for which the specified total number of inodes need to be processed.

**[-inode-percentage-complete <integer>]** - Percentage Complete

This specifies the free disk space estimates for splitting the FlexClone volumes for which the specified percentage of Inode processing has been completed.

**[-blocks-scanned <integer>]** - Blocks Scanned

This specifies the free disk space estimates for splitting the FlexClone volumes for which the specified number of blocks have been scanned.

**[-blocks-updated <integer>]** - Blocks Updated

This specifies the free disk space estimates for splitting the FlexClone volumes for which the specified number of blocks have been updated.

**[-comment <text>]** - Comment

This specifies the free disk space estimates for splitting the FlexClone volumes that have the specified value for the comment field.

**[-qos-policy-group <text>]** - QoS Policy Group Name

This parameter optionally specifies which QoS policy group to apply to the FlexClone volume. The policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to the FlexClone volume, the system does not monitor and control the traffic to the volume.

## Examples

The following example displays the FlexClone split free disk space estimates for the FlexClone volumes residing on Vserver vs0.

```
cluster1::> volume clone split estimate -vserver vs0
(volume clone split estimate)
Vserver    FlexClone    Split
-----
vs0         fc_vol_1      851.5MB
            fc_vol_3      0.00B
            flex_clone1 350.3MB
            fv_2       47.00MB
            tv9        0.00B
5 entries were displayed.
```

---

## See Also

volume clone show

---

## volume clone split show

Show the status of FlexClone split operations in-progress

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone split show` command displays the progress information of all the active FlexClone volume splitting jobs. If the `-instance` option is also specified, detailed information about all splitting jobs is displayed. This command is not supported on Infinite Volumes. This command displays the following information about all FlexClone splitting jobs:

- Vserver name
- FlexClone volume name
- Number of inodes processed during clone splitting
- Total inodes to be processed during clone splitting
- Percentage of inodes processed
- Total number of blocks scanned for clone splitting
- Total number of blocks updated for clone splitting

### Parameters

{ **[-fields <fieldname>, ...]**

This specifies the fields to be displayed, for all the ongoing FlexClone splitting jobs.

| **[-instance ]** }

This specifies the command to display detailed information about the ongoing FlexClone volume splitting jobs.

**[-vserver <vserver name>]** - Vserver Name

This specifies the command to display information about the ongoing FlexClone volume splitting jobs for all FlexClone volumes on this Vserver.

**[-flexclone <volume name>]** - FlexClone Volume

This specifies the command to display information about ongoing FlexClone volume splitting jobs for this FlexClone volume.

**[-inodes-processed <integer>]** - Inodes processed

This specifies the command to display information about all the ongoing FlexClone splitting jobs which have the specified number of Inodes processed.

**[-inodes-total <integer>]** - Total Inodes

This specifies the command to display information about all the ongoing FlexClone splitting jobs that have the specified number of total Inodes to be processed.

**[-inode-percentage-complete <integer>]** - Percentage complete

This specifies the command to display information about all the ongoing FlexClone splitting jobs that have the specified percentage of Inode processing completed.

**[-blocks-scanned <integer>]** - Blocks Scanned

This specifies the command to display information about all the ongoing FlexClone splitting jobs that have the specified number of blocks scanned.

**[-blocks-updated <integer>]** - Blocks Updated

This specifies the command to display information about all the ongoing FlexClone splitting jobs that have the specified number of blocks updated.

## Examples

The following example displays information about all the ongoing FlexClone splitting jobs in the cluster.

```
cluster1::> volume clone split show
(volume clone split show)
```

Vserver	FlexClone	Inodes		Blocks		
		Processed	Total	Scanned	Updated	% Complete
vs1	fc_vol_1	0	1260	0	0	0

The following example displays information about FlexClone volume `fc_vol_2` residing on Vserver `vs0`.

```
cluster1::> volume clone split show -vserver vs0 -flexclone fc_vol_2 -instance
(volume clone split show)
Vserver Name: vs0
FlexClone Volume: fc_vol_2
FlexClone Volume: fc_vol_2
Inodes processed: 0
Total Inodes: 3192
Percentage complete: 0
Blocks Scanned: 0
Blocks Updated: 0
```

---

## volume clone split start

Split a FlexClone from the parent volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone split start` command starts a job to separate the FlexClone volume from the underlying parent volume. Both, the parent and the FlexClone volumes will be available for the duration of the split operation. After the job starts, you can stop it using the `volume clone split stop` command. You can also stop the job using the `job stop` command. You can monitor the current progress of the job using the `volume clone split show` and `job show` commands. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver that the FlexClone volume exists on.

**-flexclone** <volume name> - FlexClone Volume

This specifies the FlexClone volume that will be split from its parent volume.

**[-foreground** [true]] - Foreground Process

This specifies whether the clone splitting job will run as a foreground job. The default value of this option is `true`.

### Examples

The following example starts splitting FlexClone volume `fc_vol_1` on Vserver `vs1` as a foreground job.

```
cluster1::> volume clone split start -vserver vs1 -flexclone fc_vol_1 -foreground true
```

### See Also

`volume clone split stop` `job stop` `volume clone split show` `job show`

---

## volume clone split stop

Stop an ongoing FlexClone split job

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume clone split stop` command stops the process of separating the FlexClone volume from its underlying parent volume, but does not lose any of the progress achieved while the split process was active. That is, all the clone volume blocks already separated from the parent volume remain separated. If you restart the split operation, splitting process begins from the beginning because no information about previously achieved progress is saved, but previously split blocks are not re-split. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver that the FlexClone volume exists on.

**-flexclone** <volume name> - FlexClone Volume

This specifies the FlexClone volume whose separation from the parent volume will be stopped.

### Examples

The following example stops an ongoing clone splitting job for FlexClone volume `fc_vol_1` on Vserver `vs1`.

```
cluster1::> volume clone split stop -vserver vs1 -flexclone fc_vol_1
```

## volume copy start

Start making a copy of a volume

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description



---

The `volume copy start` command creates a copy of the specified volume on the specified aggregate. After finishing the volume copy operation, Data ONTAP breaks the replication relationship and no relationship exists between the copy and its source volume. This command appears to run synchronously, but it actually runs asynchronously.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the `volume` is located.

**-volume** <volume name> - Volume Name

This specifies the volume that will be copied.

**-destination-volume** <volume name> - Destination Volume

This specifies the new name for the copied volume created at the destination aggregate.

**-destination-aggregate** <aggregate name> - Destination Aggregate

This specifies the aggregate to which the volume will be copied.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the volume copy operation runs as a foreground process. The default setting is `false` (that is, the operation runs in the background).

## Examples

The following example creates a copy of a volume named `vol2` that is located on a Vserver named `vs0`. The copy is named `vol2_copy1` and is stored on aggregate `aggr3`.

```
node::> volume copy start -vserver vs0 -volume vol2 -destination-volume  
vol2_copy1 -destination-aggregate aggr3
```

## volume efficiency check

Scrub efficiency metadata of a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

This command verifies and updates the fingerprint database for the specified volume. This command is not supported on Infinite Volumes that are managed by storage services.

---

## Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

Specifies the volume on which the verify operation needs to be started.

| **-path** </vol/volume> } - Volume Path

Specifies the volume path on which the verify operation needs to be started.

[**-delete-checkpoint** | **-d** {true|false}] - Delete Checkpoint

Deletes existing checkpoint.

## Examples

The following example runs `volume efficiency check` with `delete checkpoint` option turned on.

```
cluster1::> volume efficiency check -vserver vs1 -volume voll -delete-checkpoint
true
```

## volume efficiency modify

Modify the efficiency configuration of a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command is used to set or modify the schedule, policy and various other efficiency configuration options on a volume. This command is not supported on Infinite Volumes that are managed by storage services.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

This specifies the volume on which efficiency options need to be modified.

---

| **-path** </vol/volume> } - Volume Path

This specifies the volume path on which efficiency options need to be modified.

{ **[-schedule** <text>] - Schedule

This option is used to set and modify the schedule.

schedule is [day\_list][@hour\_list] or [hour\_list][@day\_list] or - or auto or manual

The day\_list specifies the days of the week that an efficiency operation should run. It is a list of the first three letters of the day (sun, mon, tue, wed, thu, fri, sat), separated by a comma. Day ranges such as mon-fri can also be used. The default day\_list is sun-sat. The names are not case sensitive.

The hour\_list specifies the hours of each scheduled day that an efficiency operation should run. The hour\_list is from 0 to 23, separated by a comma. Hour ranges such as 8-17 are allowed. Step values can be used in conjunction with ranges (For example, 0-23/2 means every two hours in a day). The default hour\_list is 0, i.e. at midnight of each scheduled day.

When efficiency is enabled on a volume for the first time, an initial schedule is assigned to the volume. This initial schedule is sun-sat@0, which means run once every day at midnight.

If "-" is specified, no schedule is set on the volume. The auto schedule string triggers an efficiency operation depending on the amount of new data written to the volume. The manual schedule string prevents SIS from automatically triggering any operations and disables change-logging. This schedule string can only be used on SnapVault destination volumes. The use of this schedule is mainly desirable when inline compression is enabled on a SnapVault destination volume and background processing is not necessary.

Note that schedule and policy are mutually exclusive options.

| **[-policy** <text>] } - Efficiency Policy Name

This option is used to set an efficiency policy.

Note that schedule and policy are mutually exclusive options.

**[-compression** {true|false}] - Compression

This option is used to enable and disable compression. The default value is false.

**[-inline-compression** {true|false}] - Inline Compression

This option is used to enable and disable inline compression. Inline compression can be enabled only if `compression` is enabled. The default value is false.

**[-idd** {true|false}] - Incompressible Data Detection

---

This option is used to enable and disable incompressible data detection. It can be enabled only if `compression` is enabled. The default value is `false`.

**[-quick-check-fsize <integer>]** - Compression Quick Check File Size

This option is used to modify the minimum file size (in bytes) required to attempt Quick check on a file. The default value is 500MB.

## Examples

The following examples modify efficiency options on a volume.

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -schedule sun-sat@12
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -policy policy1
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -compression true -inline-compression true -idd true
```

## volume efficiency off

Disables efficiency on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume efficiency off` command disables efficiency on a volume. This command is not supported on Infinite Volumes that are managed by storage services.

## Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver on which the volume is located.

**{ -volume** <volume name> - Volume Name

Specifies the name of the volume on which efficiency needs to be disabled.

**| -path** </vol/volume> } - Volume Path

Specifies the volume path on which efficiency needs to be disabled.

## Examples

The following examples disable efficiency on a volume:

```
cluster1::> volume efficiency off -vserver vs1 -volume vol1
```

---

```
cluster1::> volume efficiency off -vserver vs1 -path /vol/vol1
```

## volume efficiency on

Enable efficiency on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency on` command enables efficiency on a volume. The specified volume must be online. Efficiency operations will be started periodically according to a per volume schedule or policy. The `volume efficiency modify` command can be used to modify schedule and the `volume efficiency policy modify` command can be used to modify policy. You can also manually start an efficiency operation with the `volume efficiency start` command. This command is not supported on Infinite Volumes that are managed by storage services.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume on which efficiency needs to be enabled.

| **-path** </vol/volume> } - Volume Path

This specifies the volume path on which efficiency needs to be enabled.

### Examples

The following examples enable efficiency on a volume.

```
cluster1::> volume efficiency on -vserver vs1 -volume vol1
cluster1::> volume efficiency on -vserver vs1 -path /vol/vol1
```

### See Also

`volume efficiency modify` `volume efficiency policy modify` `volume efficiency start`

---

## volume efficiency revert-to

Reverts volume efficiency metadata

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `volume efficiency revert-to` command reverts the format of volume efficiency metadata for the volume to the given version of Data ONTAP. This command is not supported on Infinite Volumes that are managed by storage services.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume for which volume efficiency metadata needs to be reverted.

| **-path** </vol/volume> } - Volume Path

This specifies the volume path for which volume efficiency metadata needs to be reverted.

[**-version** <revert version>] - Revert to Version

Specifies the version of Data ONTAP to which the volume efficiency metadata needs to be formatted.

[**-delete** | **-d** {true|false}] - Delete Existing Metafile on Revert

If set to `true`, this parameter specifies that the volume efficiency metadata be deleted instead of reverting its format. By default this parameter is set to `false`.

[**-clean-up** | **-c** {true|false}] - Delete Previously Downgraded Metafiles

If set to `true`, this parameter specifies that the volume efficiency metadata already reverted using `volume efficiency revert-to` be deleted. By default this parameter is set to `false`.

### Examples

---

The following examples reverts volume efficiency metadata on a volume named vol1 located in vserver vs1 to version 8.1.

```
cluster1::> volume efficiency revert-to -vserver vs1 -volume voll -version 8.1
cluster1::> volume efficiency revert-to -vserver vs1 -path /vol/voll -version 8.1
```

## volume efficiency show

Display a list of volumes with efficiency

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency show` command displays the information about storage efficiency of volumes. The command output depends on the parameter or parameters specified. If no parameters are specified, the command displays the following information for all volumes with efficiency:

- Vserver: Vserver the volume belongs to.
- Volume: Name of the volume.
- State: Current state of efficiency on the volume (Enabled or Disabled).
- Status: Status of the efficiency on the volume. Following are the possible values:
  - Active: An efficiency operation is currently running.
  - Idle: There are no efficiency operations running.
  - Initializing: An efficiency operation is being initialized.
  - Undoing: Efficiency is being undone on the volume.
  - Pending: An efficiency operation is queued.
  - Downgrading: An efficiency operation necessary to downgrade the efficiency metafiles to a previous Data ONTAP release is active.
  - Disabled: Efficiency is disabled on the volume.

Status is not supported for Infinite Volumes and will display a value of "-"

- Progress: The progress of the current efficiency operation with information as to which stage of the efficiency process is currently in progress and how much data is processed for that stage. For example: "25 MB Scanned", "20 MB Searched",

---

"500 KB (2%) Compressed", "40 MB (20%) Done", "30 MB Verified". Progress is not supported for Infinite Volumes and will display a value of "-"

To display detailed information, run the command with the `-l` or `-instance` parameter. The detailed view provides all information in the previous list and the following additional information (fields not supported by Infinite Volumes will display a value of "-"):

- Path: Volume Path.
- Compression: Current state of compression on the volume (Enabled or Disabled).
- Inline Compression: Current state of inline compression on the volume (Enabled or Disabled).
- Incompressible Data Detection: Current state of Incompressible Data Detection on the volume (Enabled or Disabled).
- Compression Quick Check File Size: Minimum file size (in bytes) to attempt Quick Check on a file. The default value is 500MB.
- Type: Type of volume (Regular or SnapVault).
- Schedule: The schedule of efficiency operation for the volume.
- Policy: Efficiency policy for the volume.
- Minimum Blocks Shared: The minimum number of adjacent blocks in a file that can be shared.
- Blocks Skipped Sharing: Blocks skipped sharing because of the minimum block share value. This parameter is not supported on Infinite Volumes.
- Last Operation State: Status of the last operation (Success or Failure). Not supported on Infinite Volumes.
- Last Successful Operation Begin: The time and date at which the last successful operation began. This parameter is not supported on Infinite Volumes.
- Last Successful Operation End: The time and date at which the last successful operation ended. This parameter is not supported on Infinite Volumes.
- Last Operation Begin: The time and date at which the last operation began. This parameter is not supported on Infinite Volumes.
- Last Operation End: The time and date at which the last operation ended. This parameter is not supported on Infinite Volumes.
- Last Operation Size: The size of the last operation. This parameter is not supported on Infinite Volumes.



- 
- Last Operation Error: The error encountered by the last operation. This parameter is not supported on Infinite Volumes.
  - Change Log Usage: The percentage of the change log that is used. This parameter is not supported on Infinite Volumes.
  - Logical Data: The total logical data in the volume, and how much is reached compared to the deduplication logical data limit. This parameter is not supported on Infinite Volumes.
  - Queued Job: The job that is queued. Following are the possible values:
    - -: There are no queued jobs.
    - scan: A job to process existing data is queued.
    - start: A job to process newly added data is queued.
    - check: A job to eliminate stale data from the fingerprint database is queued.
    - downgrading: An efficiency operation necessary to downgrade the efficiency metafiles to a previous Data ONTAP release is queued.
  - Stale Fingerprints: The percentage of stale entries in the fingerprint database. If this is greater than 20 percent a subsequent `volume efficiency start` operation triggers the verify operation, which might take a long time to complete. This parameter is not supported on Infinite Volumes.

You can specify additional parameters to display information that matches only those parameters. For example, to display information only about volumes with efficiency in Vserver `vs1`, run the command with the `-vservers vs1` parameter.

No information is displayed for Infinite Volumes that are managed by storage services.

## Parameters

{ [-fields <fieldname>, ...]

This specifies the fields that need to be displayed. The fields Vserver and volume name are the default fields.

| [-l]

This option displays detailed information about the volumes with efficiency.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

---

**[-vserver <vserver name>]** - Vserver Name

Displays information only for those volumes that match the specified Vserver.

**{ [-volume <volume name>] }** - Volume Name

Displays information only for those volumes that match the specified volume.

**| [-path </vol/volume>] }** - Volume Path

Displays information only for those volumes that match the specified volume path.

**[-state {Disabled|Enabled}]** - State

Displays information only for those volumes that match the specified state.

**[-op-status <Efficiency status>]** - Status

Displays information only for those volumes that match the specified operation status.  
This parameter is not supported on Infinite Volumes.

**[-progress <text>]** - Progress

Displays information only for those volumes that match the specified progress. This parameter is not supported on Infinite Volumes.

**[-type {Regular|SnapVault}]** - Type

Displays information only for those volumes that match the specified type of volume.

**[-schedule <text>]** - Schedule

Displays information only for those volumes that match the specified schedule.

**[-policy <text>]** - Efficiency Policy Name

Displays information only for those volumes that match the specified policy.

**[-blks-skipped-sharing <integer>]** - Blocks Skipped Sharing

Displays information only for those volumes that match the specified blocks skipped sharing. This parameter is not supported on Infinite Volumes.

**[-last-op-state <text>]** - Last Operation State

Displays information only for those volumes that match the specified last operation state. This parameter is not supported on Infinite Volumes.

**[-last-success-op-begin <text>]** - Last Success Operation Begin

Displays information only for those volumes that match the specified last successful operation begin time. This parameter is not supported on Infinite Volumes.

**[-last-success-op-end <text>]** - Last Success Operation End

---

Displays information only for those volumes that match the specified last successful operation end time. This parameter is not supported on Infinite Volumes.

**[-last-op-begin <text>]** - Last Operation Begin

Displays information only for those volumes that match the specified last operation begin time. This parameter is not supported on Infinite Volumes.

**[-last-op-end <text>]** - Last Operation End

Displays information only for those volumes that match the specified last operation end time. This parameter is not supported on Infinite Volumes.

**[-last-op-size {<integer>[KB|MB|GB|TB|PB]}]** - Last Operation Size

Displays information only for those volumes that match the specified last operation size. This parameter is not supported on Infinite Volumes.

**[-last-op-error <text>]** - Last Operation Error

Displays information only for those volumes that match the specified last operation error. This parameter is not supported on Infinite Volumes.

**[-changelog-usage <percent\_no\_limit>]** - Changelog Usage

Displays information only for those volumes that match the specified change log usage. This parameter is not supported on Infinite Volumes.

**[-logical-data-size {<integer>[KB|MB|GB|TB|PB]}]** - Logical Data Size

Displays information only for those volumes that match the specified logical data size. This parameter is not supported on Infinite Volumes.

**[-logical-data-limit {<integer>[KB|MB|GB|TB|PB]}]** - Logical Data Limit

Displays information only for those volumes that match the specified logical data limit. This parameter is not supported on Infinite Volumes.

**[-logical-data-percent <percent\_no\_limit>]** - Logical Data Percent

Displays information only for those volumes that match the specified logical data percentage. This parameter is not supported on Infinite Volumes.

**[-queued-job <text>]** - Queued Job

Displays information only for those volumes that match the specified number of queued jobs. This parameter is not supported on Infinite Volumes.

**[-stale-fingerprint-percentage <integer>]** - Stale Fingerprint Percentage

Displays information only for those volumes that match the specified stale fingerprint percentage. This parameter is not supported on Infinite Volumes.

---

### **[-compression {true|false}] - Compression**

Displays information only for those volumes that match the specified compression setting.

### **[-inline-compression {true|false}] - Inline Compression**

Displays information only for those volumes that match the specified inline compression setting.

### **[-idd {true|false}] - Incompressible Data Detection**

Displays information only for those volumes that match the specified idd setting. This parameter is not supported on Infinite Volumes.

### **[-is-constituent {true|false}] - Constituent Volume**

Displays information only for those volumes that either are or are not constituents of an Infinite Volume, depending on the value provided.

### **[-quick-check-fsize <integer>] - Compression Quick Check File Size**

Displays information only for those volumes that match the specified quick-check file size setting. This parameter is not supported on Infinite Volumes.

## **Examples**

The following example displays information about all volumes with efficiency on the Vserver named vs1:

```
cluster1::> volume efficiency show -vserver vs1
Vserver      Volume      State      Status      Progress
-----
vs1          vol1        Enabled    Idle        Idle for 22:37:53
vs1          vol2        Enabled    Idle        Idle for 22:37:53
vs1          vol3        Enabled    Idle        Idle for 22:37:49
vs1          vol4        Enabled    Idle        Idle for 22:37:53
vs1          vol5        Enabled    Idle        Idle for 22:37:53
vs1          volham      Enabled    Idle        Idle for 22:37:53
vs1          volham1     Enabled    Idle        Idle for 22:37:53
7 entries were displayed.
```

The following example displays detailed information about a volume named vol1 on a Vserver named vs1:

```
cluster1::> volume efficiency show -vserver vs1 -volume vol1
Vserver Name: vs1
Volume Name: vol1
Volume Path: /vol/vol1
State: Enabled
Status: Idle
Progress: Idle for 00:00:14
Type: Regular
Schedule: sun-sat@0
Efficiency Policy Name: -
Min Blocks Shared: 1
Blocks Skipped Sharing: 0
Last Operation State: success
Last Success Operation Begin: Mon Nov 15 20:13:26 UTC 2010
Last Success Operation End: Mon Nov 15 20:13:26 UTC 2010
```

---

```
Last Operation Begin: Mon Nov 15 20:13:26 UTC 2010
  Last Operation End: Mon Nov 15 20:13:26 UTC 2010
  Last Operation Size: 0.00B
  Last Operation Error: -
    Change Log Usage: 0%
    Logical Data Size: 156KB
    Logical Data Limit: 50.00TB
    Logical Data Percent: 0%
      Queued Job: -

  Stale Fingerprint Percentage: 0
    Compression: false
      Inline Compression: false
    Incompressible Data Detection: false
  Compression Quick Check File Size: 524288000
```

## See Also

volume efficiency start

---

## volume efficiency start

Starts efficiency operation on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `volume efficiency start` command to start an efficiency operation. The volume must be online and have efficiency enabled. If there is an efficiency operation already active on the volume, this command fails.

When the `volume efficiency start` command is issued, a checkpoint is created at the end of each stage or sub-stage, or on an hourly basis in the gathering phase. If at any point the `volume efficiency start` operation is stopped, the system can restart the efficiency operation from the execution state saved in the checkpoint. The `delete-checkpoint` parameter can be used to delete the existing checkpoint and restart a fresh efficiency operation. The checkpoint corresponding to gathering has a validity period of 24 hours. If the user knows that significant changes have not been made on the volume, then such a gatherer checkpoint whose validity has expired can be used with the help of the `use-checkpoint` parameter. There is no time restriction for checkpoints of other stages.

This command is not supported on Infinite Volumes that are managed by storage services.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

Specifies the name of the volume.

| **-path** </vol/volume> } - Volume Path

Specifies the complete path of the volume.

[**-scan-old-data** | **-s** [true]] - Scan Old Data

This option scans the file system and processes all existing data. It prompts for user confirmation before proceeding. Use the force option to suppress this confirmation.

---

{ **[-use-checkpoint | -p [true]]** - Use Checkpoint (if scanning old data)

Use the checkpoint when scanning existing data. Valid only if `scan-old-data` parameter is true.

| **[-delete-checkpoint | -d [true]]** } - Delete Checkpoint

Deletes the existing checkpoint and restarts a new `volume efficiency start` operation.

**[-qos-policy <sis\_qos>]** - QoS Policy

Specifies the qos-policy, which indicates how the efficiency operations are throttled. This option can be configured to be `background` or `best-effort`. Default value is `best-effort`. If `background` is specified, the efficiency operations are run with minimum or no impact on the data serving client operations. If `best-effort` is specified, the efficiency operations might have some impact on the data serving client operations.

**[-compression | -C [true]]** - Start Compression (if scanning old data) (privilege: advanced)

Compresses existing data. Deduplication is not run unless the dedupe option is also specified. Valid only if `scan-old-data` parameter is true.

**[-dedupe | -D [true]]** - Start Deduplication (if scanning old data) (privilege: advanced)

Deduplicates existing data on disk. Similarly, compression is not run unless the compression option is also specified. Valid only if `scan-old-data` parameter is true.

**[-build-metadata | -m [true]]** - Build metadata without sharing(if scanning old data)

Builds deduplication metadata by scanning the entire file system. You will not achieve any space savings with this option. Once the metadata is built, existing data can be shared with newly written data on subsequent deduplication runs.

**[-scan-all | -o [true]]** - Scan all the data without shared block optimization(if scanning old data)

Scans the entire file system and processes the shared blocks also. You may be able to achieve additional space savings using this option. Where as, by default the option – `scan-old-data` saves some time by skipping the shared blocks.

**[-shared-blocks | -a [true]]** - Compress Shared Blocks (if scanning old data) (privilege: advanced)

Compresses the Compression Groups that have shared blocks created by deduplication or cloning data. Valid only if `scan-old-data` parameter is true.

**[-snapshot-blocks | -b [true]]** - Compress Blocks In Snapshots (if scanning old data) (privilege: advanced)

---

Compresses data blocks locked in a Snapshot copy. Valid only if `scan-old-data` parameter is true.

**[-queue | -q [true]]** - Operation Should Be Queued

Queues an efficiency operation. It will be queued only if an operation is already in progress. Valid only if `scan-old-data` is false.

**[-force | -f [true]]** - Force Operation

Suppresses all confirmation messages.

## Examples

The following examples start efficiency on a volume:

```
cluster1::> volume efficiency start -volume voll -vserver vs1
cluster1::> volume efficiency start -scan-old-data -volume voll -vserver vs1
cluster1::> volume efficiency start -volume voll -vserver vs1 -queue -delete-checkpoint
```

## volume efficiency stat

Show volume efficiency statistics

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume efficiency stat` command displays efficiency statistics. This command is not supported on Infinite Volumes. The output depends on the parameters specified with the command. If no parameters are specified, the command displays the following efficiency statistics fields for all the volumes:

- **Vserver:** The Vserver that the volume belongs to.
- **Volume Name:** Name of the volume.
- **Allocated:** The total allocated disk space in KB in the dense volume.
- **Saving:** The total amount of savings in KB due to efficiency.
- **%Saved:** The percentage of saved space by all efficiency operations over allocated space.

To display detailed information, run the command with the `-l`, `-lv` or `-instance` parameter.



---

## Parameters

{ [-fields <fieldname>, ...]

This specifies the fields that need to be displayed. The Vserver and volume name are the default fields.

| [-instance ] }

If you specify the -instance parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

Displays statistics only for those volume(s) that match the specified Vserver.

{ [-volume <volume name>] - Volume Name

Displays statistics only for those volume(s) that match the specified volume name.

| [-path </vol/volume>] } - Volume Path

Displays statistics only for those volume(s) that match the specified volume path.

[-b [true]] - Display In Blocks

Displays usage size in 4k block counts.

[-num-compressed-inline <integer>] - Inline Compression Attempts

Displays statistics only for those volume(s) that match the specified number of Compression Groups attempted inline.

## Examples

The following example displays default efficiency statistics for all the volumes.

```
cluster1::> volume efficiency stat
Vserver      Volume      Allocated      Saving      %Saved
-----
vs0          vol0          16284324 KB      4680 KB      0%
vs1          vol1          457600 KB        18684 KB      3%
vs1          vol2          3458716 KB        0 KB          0%
vs1          vol3          965296 KB         308 KB        0%
vs1          vol4          796212 KB         60 KB         0%
vs1          vol5          3762452 KB      10236 KB      0%
vs1          volham        3888 KB          0 KB          0%
vs2          vol2          156 KB           0 KB          0%
8 entries were displayed.
```

The following example display the node statistics:

```
cluster1::> volume efficiency stat -g
Node Name:      Cluster-01
Max Efficiency Ops:      8
Max Share Blocks:      3060
Pending Efficiency Ops:  0
Running Efficiency Ops:  0
Total Configured:      9
```

---

```
Succeeded Ops:      1
Started Ops:        1
Failed Ops:         4
Deferred Ops:       0
Stopped Ops:        0
Dropped Change Logs: 16384
Change Log Generated: 37347544
Change Log Flushed:  37347544
Change Log Pending:  0
```

The following example show the detailed statistics for vol1 in Vserver vs1.

```
cluster1::> volume efficiency stat -l -vserver vs1 -volume vol1
Vserver: vs1
Path: /vol/vol1
Allocated: 16776 KB
Shared: 3212 KB
Saving: 812804 KB
%Saved: 97%
Max Refcount: 32767
Total Processed: 2150464 KB
Total Process Time: 00:29:49
Total Verify Time: -
Efficiency Files: 9
Succeeded Op: 0
Started Op: 0
Failed Op: 0
Stopped Op: 0
Deferred Op: 0
Succeeded Check Op: 0
Failed Check Op: 0
Suspended Check Op: 0
Total FP Deleted: 0
Total Sorted Blocks: 0
Overlapped Blocks: 0
Same Fingerprint: 0
Same FBN Location: 0
Same Data: 0
Same VBN: 0
Mismatched Data: 0
Same Sharing Records: 0
Max Reference Hits: 0
Staled Recipient: 0
Staled Donor: 0
File Too Small: 0
Out of Space: 0
FP False Match: 0
Mismatch By Overwrites: 0
Delino Records: 0
Unaligned Compression Blocks: 0
Additional Sharing Messages: 0
Compression Saved: 0
CGs Decompressed: 0
Partial CG Modifies: 0
Avg Decompress Time: 0
Extra CP Reads: 0
Inline Compression Attempts: 0
Background Compression Attempts: 0
Inline Compressed Blocks: 0
Background Compressed CGs: 0
Uncompressed Blocks: 0
New Partial CG Writes: 0
Decompress Disk Bad: 0
Decompress SW Bad: 0
Avg Compression Time: 0
Compression Attempts: 0
Compression Failures: 0
Poor Compression Ratio: 0
CGs Skipped Due to VBN_ZERO Policy: 0
Shared Blocks Skipped: 0
Snapshot Blocks Skipped: 0
Un-Flushed Change Logs: 0
Incompressible CGs Found By Quick Check: 0
Inline Incompressible CGs: 0
Avg Incompressible Data Quick Check Time: 0
Avg Compressible Data Quick Check Time: 0
BCE Messages Received in Exempt Domain: 0
BCE Aborts Before Compress Stage: 0
BCE Aborts Due to Stale Inode Before Compress Stage: 0
BCE Aborts Due to Invalid FBN: 0
BCE Policy Stage Entries: 0
```

---

BCE Compress Stage Entries:	0
BCE CGs Skipped Due to Overwrites in Compress Stage:	0
BCE Messages Sent to Exempt Domain:	0
BCE SetFlag Stage Entries:	0
BCE Aborts Before Post Processing:	0
BCE Aborts Due to Stale Inode Before Post Processing:	0
BCE CGs Skipped Due to Overwrites in Post Processing:	0
BCE CGs Skipped Due to No Space in Post Processing:	0

---

## volume efficiency stop

Stop efficiency operation on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `volume efficiency stop` command to stop an efficiency operation. This command is not supported on Infinite Volumes that are managed by storage services.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume on which efficiency operation needs to be stopped.

| **-path** </vol/volume> } - Volume Path

This specifies the volume path on which efficiency operation needs to be stopped.

[**-all** | **-a** [true]] - Stop All Operations

This specifies both active and queued efficiency operations to be aborted.

### Examples

The following examples stop efficiency on a volume.

```
cluster1::> volume efficiency stop -vserver vs1 -volume voll
cluster1::> volume efficiency stop -vserver vs1 -volume voll -all
```

## volume efficiency undo

Undo efficiency on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

---

## Description

Remove volume efficiency on a volume by undoing compression, removing all the block sharing relationships, and cleaning up any volume efficiency specific data structures. Any efficiency operations on the volume must be disabled before issuing this command. The volume efficiency configuration is deleted when the undo process completes. This command is not supported on Infinite Volumes that are managed by storage services.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

{ **-volume** <volume name> - Volume Name

This specifies the volume name.

| **-path** </vol/volume> } - Volume Path

This specifies the volume path.

**[-compression | -C [true]]** - Decompress The Data In The Volume

Undo the effects of compression. This requires efficiency to be disabled (by performing `volume efficiency off`).

**[-dedupe | -D [true]]** - Undo Block Sharing In The Volume

Undo the effects of deduplication. This requires efficiency to be disabled (by performing `volume efficiency off`).

**[-inode | -i <integer>]** - Inode Number To Undo Sharing

Remove the block sharings from a specified inode. This parameter is not supported on Infinite Volumes.

**[-undo-type | -t {all|wrong}]** - Selective Undo

This specifies to remove either all or only invalid block sharing. When `all` is used, all block sharings are removed. When `wrong` is used, only invalid sharings present in the volume are removed. When used along with `log` option, it logs information about all or wrong block sharings without sharing removal.

**[-log | -d [true]]** - Only Log Incorrect Savings

If `true`, information about invalid block sharing relationships will only be logged. Invalid sharings will not be removed. This option is only valid when the parameter `undo-type` is set to `wrong`.

---

## Examples

The following are examples of how to use `efficiency undo`.

```
cluster1::> volume efficiency undo -vserver vs1 -volume voll
cluster1::> volume efficiency undo -vserver vs1 -volume voll -compression true
cluster1::> volume efficiency undo -vserver vs1 -volume voll -dedup true -
compression true
```

## See Also

`volume efficiency off`

---

## volume efficiency policy create

Create an efficiency policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency policy create` creates an efficiency policy.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver on which the volume is located.

**-policy** <text> - Efficiency Policy Name

This specifies the policy name.

**[-schedule <text>]** - Job Schedule Name

This specifies the job schedule. Use `job schedule` commands to manage job schedule. Only cron job schedules are supported.

**[-duration <text>]** - Duration (Hours)

This specifies the duration that an efficiency operation can run (in hours). The possible values are "-" or a number between 1 and 999 inclusive. Default value is "-", which means no duration.

**[-enabled {true|false}]** - Enabled

This specifies whether the policy is enabled or not. The policy is enabled by default.

**[-comment <text>]** - Comment

User specified comment.

**[-qos-policy <Efficiency QoS policy>]** - QoS Policy Name

This specifies how the efficiency operations are throttled. This option can be configured to be `background` or `best-effort`. Default value is `best-effort`. If `background` is specified, the efficiency operations are run with minimum or no impact on the data serving client operations. If `best-effort` is specified, the efficiency operations might have some impact on the data serving client operations.

---

## Examples

The following example creates an efficiency policy.

```
cluster1::> volume efficiency policy create -vserver vs1 -policy policy1 -  
schedule daily -duration 100
```

## See Also

job schedule



---

## volume efficiency policy delete

Delete an efficiency policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency policy delete` command deletes an efficiency policy. An efficiency policy can be deleted only when it is not associated with any volume.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver on which the volume is located.

**-policy** <text> - Efficiency Policy Name

This specifies the policy name.

### Examples

The following example deletes an efficiency policy:

```
cluster1::> volume efficiency policy delete -vserver vs1 -policy policy1
```

## volume efficiency policy modify

Modify an efficiency policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency policy modify` command can be used to modify the policy attributes.

### Parameters

**-vserver** <vserver name> - Vserver

---

This specifies the Vserver on which the volume is located.

**-policy** <text> - Efficiency Policy Name

This specifies the policy name.

**[-schedule** <text>] - Job Schedule Name

This specifies the job schedule. Use `job schedule show` to show all the jobs.

**[-duration** <text>] - Duration (Hours)

This specifies the duration that an efficiency operation can run in hours. The possible value is between 1 and 999 inclusive.

**[-enabled** {true|false}] - Enabled

This specifies whether the policy is enabled or not. Default value is true.

**[-comment** <text>] - Comment

User specified comment.

**[-qos-policy** <Efficiency QoS policy>] - QoS Policy Name

This specifies how the efficiency operations are throttled. This option can be configured to be `background` or `best-effort`. Default value is `best-effort`. If `background` is specified, the efficiency operations are run with minimum or no impact on the data serving client operations. If `best-effort` is specified, the efficiency operations might have some impact on the data serving client operations.

## Examples

The following example modifies efficiency policy.

```
cluster1::> volume efficiency policy modify -policy policy1 -schedule hourly
```

## See Also

`job schedule show`

---

## volume efficiency policy show

Show efficiency policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume efficiency policy show` command displays information about efficiency policies. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all policies:

- Vserver: Name of the Vserver, the policy belongs to.
- Policy Name: Efficiency policy name.
- Job Schedule: Job schedule name.
- Duration (Hours): The duration in hours the efficiency operation can run.
- Enable: Whether the policy is enabled or not.
- Comment: User specified comment.

You can specify additional parameters to display information that matches only those parameters. For example, to display efficiency policies only with duration 5 hours, run the command with the `-duration 5` parameter.

### Parameters

{ **[-fields** <fieldname>, ...]

This specifies the fields that need to be displayed. The fields Vserver and policy are the default fields (see example).

| **[-instance** ] }

If this parameter is specified, the command displays information about all entries.

**[-vserver** <vserver name>] - Vserver

If this parameter is specified, the command displays information only about the policy or policies that match the specified Vserver.

**[-policy** <text>] - Efficiency Policy Name

---

If this parameter is specified, the command displays information only about the policy or policies that match the specified policy name.

**[-schedule <text>]** - Job Schedule Name

If this parameter is specified, the command displays information only about the policy or policies that match the specified schedule.

**[-duration <text>]** - Duration (Hours)

If this parameter is specified, the command displays information only about the policy or policies that match the specified duration hours.

**[-enabled {true|false}]** - Enabled

If this parameter is specified, the command displays information only about the policy or policies that have the specified enabled setting.

**[-comment <text>]** - Comment

If this parameter is specified, the command displays information only about the policy or policies that match the specified comment.

**[-qos-policy <Efficiency QoS policy>]** - QoS Policy Name

If this parameter is specified, the command displays information only about the policy or policies that match the specified throttling method. The values can be `background` or `best-effort`.

**[-policy-owner {cluster-admin|vserver-admin}]** - Policy Owner

If this parameter is specified, the command displays information only about the policy or policies that match the specified owner. The values can be `cluster-admin` or `vserver-admin`.

## Examples

The following example shows all the efficiency policies with the matching Vserver `vs1`.

```
cluster1::> volume efficiency policy show -vserver vs1
Job
Vserver  Policy Name  Schedule  Duration  Enabled  Comment
-----
vs1      policy1      daily     -         false   -
vs1      policy2      daily     -         true    -
2 entries were displayed.
```

The following example shows all the policies with the following fields - Vserver (default), policy (default) and duration.

```
cluster1::> volume efficiency policy show -fields duration
vserver policy duration
-----
vdaga    policy2 -
```

---

```
vs1      policy1 -  
vs1      policy2 -  
vs2      policy2 -  
4 entries were displayed.
```

---

## volume file modify

Manage the association of a QoS policy group with a file

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command adds and removes files from QoS policy groups. QoS policy groups define measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. A QoS policy group associated with this file can be created, modified, and deleted. You cannot associate a file to a QoS policy group if a LUN was created from the file.

### Parameters

**-vserver** <vserver name> - Vserver Managing Volume

This specifies the Vserver on which the volume (containing the file) resides.

**-volume** <volume name> - Volume Name

This specifies the name of the volume. The name must be unique within the hosting Vserver.

**-file** <text> - File Path

This specifies the actual path of the file with respect to the volume.

**-qos-policy-group** <text> - QoS Policy Group Name

This option associates the file with a QoS policy group. This policy group manages storage system resources to deliver your desired level of service. If you do not assign a policy to a file, the system will not monitor and control the traffic to it. To remove this file from a QoS policy group, enter the reserved keyword “none”.

### Examples

```
cluster1::> vol file modify -vserver vs0 -volume vs0_vol156 -file 1.txt -qos-  
policy-group fast
```

Associates the file 1.txt with the fast QoS policy group.

---

## volume file reservation

Get/Set the space reservation info for the named file.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume file reservation` command can be used to query the space reservation settings for the named file, or to modify those settings. This command is not supported on Infinite Volumes. With no further modifiers, the command will report the current setting of the space reservation flag for a file. This tells whether or not space is reserved to fill holes in the file and to overwrite existing portions of the file that are also stored in a snapshot. For symlinks, the link is followed and the command operates on the link target.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver on which the volume is located. If only one data Vserver exists, you do not need to specify this parameter.

**-path** <path> - File Name

Specifies the complete file path for which we want to get/set the space reservation settings.

**[-is-enabled <text>]** - enable | disable

Specifying enable or disable will turn the reservation setting on or off accordingly for the file.

### Examples

The following example enables the file reservation setting for the file named file1. The file file1 is stored in volume testvol on Vserver vs0.

```
node::> file reservation -vserver vs0 /vol/testvol/file1 enable
space reservations for file /vol/testvol/file1: on.
```

## volume file show-disk-usage

---

Show disk usage of file

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command requires a path to a file in a volume and displays the following information:

- Vserver name
- Total bytes used by the file in kilobytes
- Full Path to the file

If not logged in as Vserver administrator, the command also requires a Vserver name. This command is not supported on an Infinite Volume.

Note:

The "-instance" option provides the same result as the default as there are no extra fields to display.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-h ]

If this parameter is specified, the command displays total bytes used by the file in human readable form.

| [-k ]

If this parameter is specified, the command displays total bytes used by the file in kilobytes.

| [-m ]

If this parameter is specified, the command displays total bytes used by the file in megabytes.

| [-u ]



---

If this parameter is specified, the command displays the unique bytes used by the file (bytes that are not shared with any other file in the volume due to deduplication or FlexClone files) in kilobytes.

| [-uh ]

If this parameter is specified, the command displays the unique bytes used by the file in human readable form.

| [-uk ]

If this parameter is specified, the command displays the unique bytes used by the file in kilobytes.

| [-um ]

If this parameter is specified, the command displays the unique bytes used by the file in megabytes.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**-vserver** <vserver name> - Vserver

This parameter is used to specify the Vserver that contains the file for which the command displays the total bytes used. It is required if not logged in as Vserver administrator.

**-path** </vol/<volume name>/<file path>> - Full Path

This required parameter is used to specify the path of the file for which the command displays the total bytes used.

**[-range | -r <<start offset>:<end offset>>]** - Block Range

If this parameter is specified, the command displays the total bytes used by the file in the specified block range.

## Examples

The following example displays the disk-usage of the file `file1.txt` in volume `/vol/root_vs0`.

```
cluster1::> volume file show-disk-usage -vserver vs0 -path /vol/root_vs0/
file1.txt

Vserver          Total          Path
-----
vs0              1408KB        /vol/root_vs0/file1.txt
cluster1::> volume file show-disk-usage -m -vserver vs0 -path /vol/root_vs0/
file1.txt

Vserver          Total          Path
-----
```

---

```
vs0          1MB          /vol/root_vs0/file1.txt
vs0::> volume file show-disk-usage -um -path /vol/root_vs0/file1.txt

Vserver      Total        Unique        Path
-----
vs0          1MB          1MB          /vol/root_vs0/file1.txt
```

---

## volume file show-filehandle

Show the file handle of a file

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command requires a path to a file in a volume and displays the file handle information described below:

- Vserver name
- Path to the file
- File handle flags
- Snapshot ID of the file (snapid)
- File ID
- File handle generation number
- File system ID (fsid)
- Master data set ID (msid)
- Data set ID (dsid)

If not logged in as a Vserver administrator, the command also requires a Vserver name.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver Managing Volume

This specifies the Vserver where the file resides.

---

**[-path <text>]** - Path to File

This specifies the path to the file.

**Examples**

The following example displays the file handle information of a file named file1.txt in the volume /vol/vol1.

```
cluster1::> volume file show-filehandle -vserver vs0 -path /vol/vol1/file1.txt
      Vserver      Path
-----
      vs0          /vol/vol1/file1.txt

dsid      flags      snapid      fileid      generation      fsid      msid
-----
0x402      0x0        0          0x60        0x206b6         0x402      0x80000402
```

---

## volume file clone autodelete

Enable/Disable autodelete

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume file clone autodelete` command enables or disables the automatic deletion of a LUN clone. Newly created LUN clones are enabled for automatic deletion by default. This command is not supported on Infinite volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume resides. If only one data Vserver exists, you do not need to specify this parameter.

**[-volume** <volume name>] - Volume Name

This specifies the name of the volume in which the LUN is present.

**-clone-path** <text> - Clone Path

This specifies the path where clone resides. If you use the volume parameter, then specify the relative path to the LUN clone. Otherwise, specify the absolute path.

**-enable** {true|false} - Enable Autodelete

This parameter enables or disables the autodelete feature for the LUN clones in the specified volume.

### Examples

The following command enables for automatic deletion a LUN Clone named `lun_clone` contained in a volume named `volume1`. This volume is present on a Vserver named `vs1`.

```
cluster1::> volume file clone autodelete /vol/volume1/lun_clone -enable true -  
vserver vs1
```

The following command specifies the relative clone path when the volume parameter is specified in the command.

```
cluster1::> volume file clone autodelete lun_clone -enable true  
-vserver vs1 -volume volume1
```

---

## volume file clone clear

Clears information of a failed clone operation

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `volume file clone clear` command is deprecated from 8.1 onwards.

### Parameters

None

### Examples

---

## volume file clone create

Create file or LUN full or sub file clone

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume file clone create` command creates a clone of a file or a LUN. This command is not supported on Infinite Volumes. You can optionally specify the following parameters for the clone file creation process:

- Vserver in which the volume resides
- Name of the parent snapshot
- The range of blocks to be cloned
- The option to avoid space reservations for the new file or LUN clone
- The option to assign a QoS policy group to the new file or LUN clone

File or LUN clones create a duplicate copy of another file or LUN, but don't require copying the data itself. This allows the clone operation to occur in constant time, taking the same amount of time to complete no matter the size of the file being cloned. This also means that clones require only a small amount of additional storage space because the clone shares the data with the source file or LUN.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver in which the parent volume resides. If only one data Vserver exists, you do not need to specify this parameter.

**[-volume** <volume name>] - Volume

This specifies the name of volume in which a file or LUN is going to be cloned.

**-source-path** <text> - Source Path

This specifies the path to the file or LUN to be cloned relative to the specified volume.

**-destination-path** <text> - Destination Path

This specifies the path for the newly-created cloned file or LUN relative to the specified volume. If the file or LUN clone to be created is a whole file or LUN ,the destination file

---

or LUN must not exist. If the `range` parameter is being specified the destination file or LUN must exist.

**[-snapshot-name | -s <snapshot name>]** - Source Snapshot

The name of the Snapshot copy to use as the source for the clone operation. If this value is not specified, the active filesystem will be used instead.

**{ [-range | -r <text>, ...]** - Block Range

This specifies the block range to be cloned. If the range is not specified, the entire file or LUN is cloned. The block range should be specified in the format `s:d:n` where `s` is the source start block number, `d` is the destination start block number, and `n` is the length in blocks to be cloned. If this parameter is used the path provided by the `destination-path` parameter must refer to a file or LUN which already exists. If either the source or destination are a LUN then the block size is measured in 512-byte LBA blocks. If neither the source nor destination are a LUN then the block size will be 4KB. If 512-byte sectors are used the source and destination offsets must have the same offset within 4KB blocks.

This option is most likely to be used by external automated systems in managing virtual disk configurations and not by human administrators.

**| [-no-reserve | -o [true]] }** - Do not reserve clone

If this option is used the clone file or LUN will not be guaranteed space in the underlying aggregate. While this out-of-space condition persists, writes to the clone file or LUN would fail. This option may be useful if few writes to the clone are expected to be needed, or to allow a file or LUN clone to be created under space-constrained conditions for recovery purposes. If this option is not specified the clone will inherit the space reservation properties from the source.

**[-ignore-streams | -i [true]]** - Ignore streams

This parameter specifies whether streams should be ignored during cloning of files or LUNs. If you set this parameter to `FALSE`, the streams are ignored; otherwise, they are included in the clones. The default value is `FALSE`.

**[-ignore-locks | -k [true]]** - Ignore locks

This parameter specifies whether byte-range locks and shared-mode locks on files or LUNs should be ignored during cloning. If you set this parameter to `TRUE`, the locks are ignored; otherwise, clone operation fails if locks are present on files or LUNs. The default value is `FALSE`.

**[-qos-policy-group <text>]** - QoS Policy Group Name

This optionally specifies which QoS policy group to apply to the file or LUN. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group



---

to a file or LUN, the system will not monitor and control the traffic to it. You cannot associate a file to a QoS policy group if a LUN was created from the file.

## Examples

The following command creates a FlexClone file of the file named myfile contained in a volume named vol. The file myfile is located in the root directory of that volume. The cloned file myfile\_copy resides in the root directory same volume.

```
cluster1::> volume file clone create -volume vol -source-path /myfile -  
destination-path /myfile_copy
```

The following command optionally associates the FlexClone file named myfile\_copy with the fast QoS policy group.

```
cluster1::> volume file clone create -volume vol -source-path /myfile -  
destination-path /myfile_copy -qos-policy-group fast
```

## volume file clone status

Gets the status of running and failed clone operations

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The `volume file clone status` command is deprecated from 8.1 onwards.

## Parameters

None

## Examples

---

## volume file clone stop

Stops a running clone operation

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `volume file clone stop` command is deprecated from 8.1 onwards.

### Parameters

None

### Examples

---

## volume flexcache create

Cache a volume throughout the cluster

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows an admin to enable caching for a volume in the cluster. This is done by creating a cache volume on every node, using the aggregate with the most free space. The choice is limited to only the aggregates to which the given admin has access. A warning message is issued if the command is unable to create a cache volume on a node, and the other cache volumes created are not deleted. All cache volumes created by this interface can also be managed through the volume interface. This command is idempotent. If a cache volume already exists on a node, no additional cache volumes are created. This command needs to be reissued if new nodes are added, and caching needs to be enabled on those nodes. This command may also need to be reissued if aggregates are moved between nodes. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver in which the cache (and origin) volumes reside.

**-origin-volume** <volume name> - Origin Volume Name

This specifies the origin volume that is the authoritative source of data. The origin must be a RW or DP volume and must not have load-sharing mirrors configured.

### Examples

The following example creates cache volumes on every node of Vserver vs1 for origin volume origin. The output of this command contains one line for each cache volume that is created successfully. If there is insufficient space in any suitable aggregate on a node, creation of a cache volume fails.

```
cluster1::> volume flexcache create -vserver vs1 -origin-volume origin
Successfully created cache volume "origin_cache_node01_aggr" in aggregate
"node01_aggr".
Successfully created cache volume "origin_cache_node02_aggr" in aggregate
"node02_aggr".
The origin volume "origin" is now cached on all qualifying aggregates in the
cluster.
```



---

## volume flexcache delete

Delete caching for a given volume throughout the cluster

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows an admin to disable caching of a volume in the cluster. This is done by deleting all cache volumes for this origin, whether they were created by a `volume flexcache create` or `volume create` command. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver in which the cache (and origin) volumes reside.

**-origin-volume** <volume name> - Origin Volume Name

This specifies the origin volume that is the authoritative source of data.

### Examples

The following example deletes all cache volumes for origin volume origin on Vserver vs1. If a node is down, the cache volume on that node is not deleted. You must manually delete such cache volumes.

```
cluster1::> volume flexcache delete -vserver vs1 -origin-volume origin
Successfully deleted cache volume "origin_cache_node01_aggr".
Successfully deleted cache volume "origin_cache_node02_aggr".
The origin volume "origin" is no longer cached in the cluster.
```

### See Also

`volume flexcache create` `volume create`

---

## volume flexcache show

Display cluster-wide caches

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the FlexCache configuration and volume state for cache volumes and their origins. This command is not supported on Infinite Volumes.

### Parameters

{ [-**fields** <fieldname>, ...]

If this parameter is used, the command displays only the fields that you specify.

| [-**instance** ] }

If this parameter is specified, the command displays detailed information about the cache volumes.

[-**vserver** <vserver name>] - Vserver

If this parameter and the `-cache-volume` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information only about the cache volumes on the specified Vserver.

[-**cache-volume** <volume name>] - Cache Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed information about the specified volume. If this parameter is specified by itself, the command displays information only about the cache volumes matching the specified name.

[-**origin-volume** <volume name>] - Origin Volume Name

If this parameter is specified, the command displays information only about the cache volumes that have the specific origin volume.

[-**cache-aggregate** <aggregate name>] - Cache Aggregate Name

If this parameter is specified, the command displays information only about the cache volumes that reside on the specified storage aggregate.

---

**[-cache-size {<integer>[KB|MB|GB|TB|PB]]} - Cache Volume Size**

If this parameter is specified, the command displays information only about the cache volumes that have the specified size. The size is specified as a number followed by a unit designation: KB (Kilobytes), MB (Megabytes), GB (Gigabytes), TB (Terabytes), or PB (Petabytes). If the unit designation is not specified, bytes are used as the unit, and the specified number is rounded up to the nearest 4 KB.

**[-cache-state {online|restricted|offline|force-online|force-offline|mixed}] - Cache Volume State**

If this parameter is specified, the command displays information only about the cache volumes that have the specified state. Possible values are:

- online: The cache volume is online.
- offline: The cache volume is offline.
- restricted: Data access to the cache volume is restricted.

**[-cache-available {<integer>[KB|MB|GB|TB|PB]]} - Cache Available Size**

If this parameter is specified, the command displays information only about the cache volumes that have the specified available size.

**[-cache-percent-used <integer>] - Cache Used Percentage**

If this parameter is specified, the command displays information only about the cache volumes that have the specified used percentage.

**[-cache-node {<nodename>|local}] - Cache Node Name**

If this parameter is specified, the command displays information only about the cache volumes that reside on the specified cluster node.

**[-connection-status <text>] - Connection Status Between Cache and Origin**

If this parameter is specified, the command displays information only about the cache volumes that have the specified connection-status. Possible values are:

- ok: The origin volume is connected and online.
- offline: The origin volume is offline.
- disconnected: Not connected to the origin volume.
- quiesced: The origin volume is in quiescing or quiesced state.

**[-origin-aggregate <aggregate name>] - Origin Aggregate Name**

If this parameter is specified, the command displays information only about the cache volumes whose origins reside on the specified storage aggregate.

**[-origin-state {online|restricted|offline|force-online|force-offline|mixed}]** - Origin Volume State

If this parameter is specified, the command displays information only about the cache volumes whose origins have the specified state. Possible values are:

- online: The origin volume is online.
- offline: The origin volume is offline.
- restricted: Data access to the origin volume is restricted.

**[-origin-node {<nodename>|local}]** - Origin Volume Node Name

If this parameter is specified, the command displays information only about the cache volumes whose origins reside on the specified cluster node.

## Examples

The following example displays configuration and volume state information for all the cache volumes and their respective origin volumes in the Vserver:

```
cluster1::> volume flexcache show
```

Vserver	-----Cache-----				Conn.- Status	-----Origin-----			
	Volume	Aggregate	Size	State		Available	Volume	Aggregate	State
vs1	dst_cache_01								
		node01_aggr	20MB	online	19.91MB	ok	dst	node02_aggr	online
	dst_cache_02								
		node02_aggr	20MB	online	19.91MB	ok	dst	node02_aggr	online
	origin_cache_node01_aggr								
		node01_aggr	20MB	online	19.91MB	ok	origin	node01_aggr	online
	origin_cache_node02_aggr								
		node02_aggr	20MB	online	19.91MB	ok	origin	node01_aggr	online
	src_cache_01								
		node01_aggr	20MB	online	19.90MB	ok	src	node01_aggr	online



---

## volume flexcache cache-policy create

Add a new cache policy

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

This command creates a cache policy in the Vserver. The default policy is a special cache policy that is created when a new Vserver is created, and deleted when a Vserver is deleted. It can be modified, but not deleted.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the Vserver of the cache policy.

**-policy** <cache policy> - Cache Policy Name

This specifies the name of the cache policy.

**-reg-ttl** <integer> - Regular File TTL in Seconds

This specifies the optional value of regular file TTL in seconds. This value determines the maximum amount of staleness that the cache allows for all inode types other than the directory type. The default is 0 seconds.

**-dir-ttl** <integer> - Directory File TTL in Seconds

This specifies the optional value of directory file TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes of the directory type. The default is 0 seconds.

**[-meta-ttl <integer>]** - ONTAP Metafile TTL in Seconds

This specifies the optional value of ONTAP metafile TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes that are internal ONTAP metafiles. The default is 15 seconds.

**[-sym-ttl <integer>]** - Symbolic Link TTL in Seconds

This specifies the optional value of symbolic link TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes that are symbolic links. The default is 0 seconds.

---

**[-other-ttl <integer>]** - Other File TTL in Seconds

This specifies the optional value of other file TTL in seconds. This is a catch-all that determines the maximum amount of staleness that the cache allows for inodes that are not symbolic links, ontap metafiles, directories, or normal files. The default is 0 seconds.

**[-deleg-lru-timeout <integer>]** - Delegation LRU Timeout in Seconds

This specifies the optional value of delegations LRU timeout in seconds. This determines the LRU timeout for FlexCache delegations, after which the Cache considers the delegation unused and returns it to the Origin. The default is 3600 seconds (1 hour).

**[-prefer-local-cache {true|false}]** - Prefer Local Cache

This specifies the optional value of prefer local cache. If a cache and its origin volume reside on the local node, this determines if cache volume should be preferred over the origin for serving any client requests. The default value is false.

## Examples

The following example creates a cache policy named strict in the Vserver vs1 with TTL values of 0 for all file types, a delegations LRU value of 300 and a preference for local cache in serving client requests:

```
cluster1::> volume flexcache cache-policy create -vserver vs1 -policy strict
-reg-ttl 0 -dir-ttl 0 -meta-ttl 0 -sym-ttl 0 -other-ttl 0 -deleg-lru-timeout 300
-prefer-local-cache true
```

---

## volume flexcache cache-policy delete

Delete a cache policy

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

This command deletes a cache policy in the Vserver. The default policy is a special cache policy that is created when a new Vserver is created, and deleted when a Vserver is deleted. It can be modified, but not deleted.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the Vserver of the cache policy.

**-policy** <cache policy> - Cache Policy Name

This specifies the name of the cache policy.

### Examples

The following example deletes a cache policy named strict in the Vserver vs1:

```
cluster1::> volume flexcache cache-policy delete -vserver vs1 -policy strict
```

## volume flexcache cache-policy modify

Modify a cache policy

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

This command modifies a cache policy in the Vserver. The default policy is a special cache policy that is created when a new Vserver is created, and deleted when a Vserver is deleted. It can be modified, but not deleted.

### Parameters

---

**-vserver** <vserver> - Vserver

This specifies the Vserver of the cache policy.

**-policy** <cache policy> - Cache Policy Name

This specifies the name of the cache policy.

**[-reg-ttl <integer>]** - Regular File TTL in Seconds

This specifies the optional value of regular file TTL in seconds. This determines the maximum amount of staleness that the cache allows for all inode types other than the directory type. The default is 0 seconds.

**[-dir-ttl <integer>]** - Directory File TTL in Seconds

This specifies the optional value of directory file TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes of the directory type. The default is 0 seconds.

**[-meta-ttl <integer>]** - ONTAP Metafile TTL in Seconds

This specifies the optional value of ONTAP metafile TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes that are internal ONTAP metafiles. The default is 15 seconds.

**[-sym-ttl <integer>]** - Symbolic Link TTL in Seconds

This specifies the optional value of symbolic link TTL in seconds. This determines the maximum amount of staleness that the cache allows for inodes that are symbolic links. The default is 0 seconds.

**[-other-ttl <integer>]** - Other File TTL in Seconds

This specifies the optional value of other file TTL in seconds. This is a catch-all that determines the maximum amount of staleness that the cache allows for inodes that are not symbolic links, ontap metafiles, directories, or normal files. The default is 0 seconds.

**[-deleg-lru-timeout <integer>]** - Delegation LRU Timeout in Seconds

This specifies the optional value of delegations LRU timeout in seconds. This determines the LRU timeout for FlexCache delegations, after which the Cache considers the delegation unused and returns it to the Origin. The default is 3600 seconds (1 hour).

**[-prefer-local-cache {true|false}]** - Prefer Local Cache

This specifies the optional value of prefer local cache. If a cache and its origin volume reside on the local node, this determines if cache volume should be preferred over the origin for serving any client requests. The default value is false.

---

## Examples

The following example modifies a cache policy named strict in the Vserver vs1 so that it now has TTL values of 5, 10, 5, 0, 15 for regular files, directories, metafiles, symbolic links, and other files respectively. In addition, the cache policy has a delegations LRU value of 100 and a preference for local cache in serving client requests:

```
cluster1::*> volume flexcache cache-policy modify -vserver vs1 -policy strict  
-reg-ttl 5 -dir-ttl 10 -meta-ttl 5 -sym-ttl 0 -other-ttl 15 -deleg-lru-timeout  
100 -prefer-local-cache true
```

---

## volume flexcache cache-policy show

Display the cache policies

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

This command shows cache policies for all the Vservers.

### Parameters

{ [-**fields** <fieldname>, ...]

If this parameter is used, the command displays only the fields that you specify.

| [-**instance** ] }

If this parameter is specified, the command displays information about all entries.

[-**vserver** <vserver>] - Vserver

If this parameter is specified, the command displays detailed information about cache policies for the specified Vserver.

[-**policy** <cache policy>] - Cache Policy Name

If this parameter is specified, the command displays detailed information about all cache policies matching this cache-policy name.

[-**reg-ttl** <integer>] - Regular File TTL in Seconds

If this parameter is specified, the command displays detailed information about all cache policies matching this reg-ttl value.

[-**dir-ttl** <integer>] - Directory File TTL in Seconds

If this parameter is specified, the command displays detailed information about all cache policies matching this dir-ttl value.

[-**meta-ttl** <integer>] - ONTAP Metafile TTL in Seconds

If this parameter is specified, the command displays detailed information about all cache policies matching this meta-ttl value.

[-**sym-ttl** <integer>] - Symbolic Link TTL in Seconds

---

If this parameter is specified, the command displays detailed information about all cache policies matching this sym-ttl value.

**[-other-ttl <integer>]** - Other File TTL in Seconds

If this parameter is specified, the command displays detailed information about all cache policies matching this other-ttl value.

**[-deleg-lru-timeout <integer>]** - Delegation LRU Timeout in Seconds

If this parameter is specified, the command displays detailed information about all cache policies matching this deleg-lru-timeout value.

**[-prefer-local-cache {true|false}]** - Prefer Local Cache

If this parameter is specified, the command displays detailed information about all cache policies matching this prefer-local-cache value.

## Examples

The following example displays cache policies that have reg-ttl values of 0 for Vserver vs1:

```
cluster1::> volume flexcache cache-policy show -vserver vs1 -reg-ttl 0
(volume flexcache cache-policy show)
Vserver  Policy      File      Dir      Meta      Symbol  Other  Delegation  Prefer
-----  -
vs1      default      0         0         15        0       0       3600        false
         strict      0         1         1         1       0       100         true
2 entries were displayed.
```

The following example displays cache policies for all Vservers:

```
cluster1::> volume flexcache cache-policy show
(volume flexcache cache-policy show)
Vserver  Policy      File      Dir      Meta      Symbol  Other  Delegation  Prefer
-----  -
vs1      default      0         0         15        0       0       3600        false
         ease       15        15        45        45      100     3600        true
         strict      0         1         1         1       0       100         true
vs2      cpl         1         2         5         10      10       60         false
         default      0         0         15        0       0       3600        false
5 entries were displayed.
```

---

# volume move abort

Stop a running volume move operation

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

The "volume move abort" command sends an abort message to the volume move operation and returns immediately. The volume move operation might not abort immediately depending on the stage it is in. For example, if the volume move operation is in a cut-over or clean-up phase, the abort is ignored. You invoke the "volume move show" command to view the list of running volume move operations and monitor the progress of the abort operation. This command has the same behavior as the `job stop -id <job-id>` command where the job-id is the identifier of the volume move job.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the name of the volume being moved.

## Examples

The following example aborts running volume move operation on volume vol1

```
Complete cluster::> volume move show
Vserver   Volume   State   Move Phase Percent-Complete Time-To-
-----
vs0       vol1     alert   cutover_hard_deferred 0% -
vs0       vol2     failed  failed -
2 entries were displayed.

cluster::> volume move abort -vserver vs0 -volume vol1
status cluster::> volume move show -vserver vs0 -volume vol1 -fields completion-
vserver volume completion-status
-----
vs0       vol1     "Volume move job stopped."
```



The following example shows command failed to abort on vol2 as volume move operation is completed.

```
cluster::> volume move show
Complete  Vserver      Volume      State      Move Phase Percent-Complete Time-To-
-----
vs0       vol1         alert      cutover_hard_deferred 0%      -
vs0       vol2         failed     failed      -
2 entries were displayed.

cluster::> volume move abort -vserver vs0 -volume vol2
Error: command failed: There is no volume move operation running on the
specified volume.
```

See Also

job stop

---

## volume move show

Show status of a volume moving from one aggregate to another aggregate

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The volume move show command displays information about volume moves in the cluster. By default, with no parameters, it only shows volume moves that have failed or are currently running. The command display output depends on the parameters passed. If no parameters are passed, the following information is displayed:

- Vserver Name: The Vserver on which the volume is located.
- Volume Name: The volume that is part of a completed or running volume move operation.
- Actual Completion Time: The date and time in the cluster time zone when the volume move completed.
- Specified Action For Cutover: The action to be taken for cutover or during cutover failure. This is the input given during the start of volume move.
- Specified Cutover Attempts: The number of attempts to be used by the move operation to cutover to the destination volume. This is the input given during the start of volume move.
- Specified Cutover Time Window: The time window in seconds given as an input for the cutover phase of volume move. This is the input given during the start of volume move.
- Time Cutover was Triggered: The time when move operation last accepted a trigger to initiate cutover. This is applicable when the move operation is waiting for a cutover to be triggered because of a hard cutover deferred state or because the cutover-action was wait.
- Time Cutover was last triggered: The time when the move operation initiated cutover.
- Destination Aggregate: The name of the aggregate to which the volume is moved.
- Detailed Status: The detail about any warnings, errors, and state of the move operation.

- 
- **Estimated Time of Completion:** The approximate date and time in the cluster time zone when the entire volume move operation is expected to complete. Note that this time may keep increasing when the move goes into cutover-deferred mode. In those cases where the input for cutover-action is wait, during the data copy phase, the estimated time of completion will approximate the time to reach the cutover point and wait for user intervention.
  - **Managing Node:** The node in the cluster on which the move job is or was running. This is usually on the node hosting the volume to be moved.
  - **Percentage Complete:** The amount of work to move the volume completed thus far in terms of percentage.
  - **Move Phase:** The phase of the move operation.
  - **Estimated Remaining Duration:** The approximate amount of time in terms of days, hours, minutes and seconds remaining to complete the volume move.
  - **Replication Throughput:** The current replication throughput of the move operation in terms of Kb/s, Mb/s or Gb/s.
  - **Duration of Move:** The duration in days, hours and minutes for which the volume move was or is in progress.
  - **Source Aggregate:** The name of the aggregate where the volume being moved originally resides or resided.
  - **Start Time of Move:** The date and time in the cluster time zone when the volume move operation started.
  - **Move State:** The state of the volume move at the time of issuing the command and the system gathering up the information about the move.

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver Name

This specifies the Vserver on which the volume is located. If this parameter and the `-volume` parameter are specified, the command displays detailed information about

---

latest move performed on the specified volume. If this parameter is specified by itself, the command displays information about latest moves performed on volumes of the specified Vserver.

**[-volume <volume name>]** - Volume Name

This specifies the volume that is part of a completed or running volume move operation. If this parameter and the `-vserver` parameter are specified, the command displays detailed information about latest move performed on the specified volume. If this parameter is specified by itself, the command displays information about the latest move on all volumes matching the specified name.

**[-actual-completion-time <Date>]** - Actual Completion Time

If this parameter is specified, the command displays move operations that match the specified date and time in the cluster time zone when the volume move completed.

**[-cutover-action {abort\_on\_failure|defer\_on\_failure|force|wait}]** - Specified Action For Cutover

If this parameter is specified, the command displays move operations that match the specified action to be taken for cutover or during cutover failure.

**[-cutover-attempts <integer>]** - Specified Cutover Attempts

If this parameter is specified, the command displays move operations that match the specified number of attempts to be used by the move operation to cutover to the destination volume.

**[-cutover-window <integer>]** - Specified Cutover Time Window

If this parameter is specified, the command displays move operations that match the specified time window in seconds for the cutover phase of volume move.

**[-cutover-trigger-time <Date>]** - Time User Triggered Cutover

If this parameter is specified, the command displays move operations that match the specified time when move operation last accepted a trigger to initiate cutover.

**[-last-cutover-trigger-time <Date>]** - Time Move Job Last Entered Cutover

If this parameter is specified, the command displays move operations that match the specified time when move operation initiated cutover.

**[-destination-aggregate <aggregate name>]** - Destination Aggregate

If this parameter is specified, the command displays move operations that match the specified name of the aggregate to which the volume is being moved.

**[-details <text>]** - Detailed Status

---

If this parameter is specified, the command displays move operations that match the specified detail about any warnings, errors and state of the move operation.

**[-estimated-completion-time <Date>]** - Estimated Time of Completion

If this parameter is specified, the command displays move operations that match the specified date and time in the cluster time zone when the entire volume move operation is expected to complete.

**[-managing-node <nodename>]** - Managing Node

If this parameter is specified, the command displays move operations that match the specified node in the cluster on which the move job is or was running.

**[-percent-complete <percent>]** - Percentage Complete

If this parameter is specified, the command displays move operations that match the specified the amount of work to move the volume completed thus far in terms of percentage.

**[-phase {queued|initializing|replicating|cutover|cutover\_hard\_deferred|cutover\_soft\_deferred|aborting|completed|cleaning\_up|failed|restarting}]** - Move Phase

If this parameter is specified, the command displays move operations that match the specified phase of the move operation.

**[-prior-issues <text>]** - Prior Issues Encountered (privilege: advanced)

If this parameter is specified, the command displays move operations that match the specified issues or transient errors encountered causing the move operation to retry the data copy phase or the cutover phase.

**[-estimated-remaining-duration <timeticks>]** - Estimated Remaining Duration

If this parameter is specified, the command displays move operations that match the specified time in terms of days, hours, minutes and seconds remaining to complete the volume move.

**[-replication-throughput <text>]** - Replication Throughput

If this parameter is specified, the command displays move operations that match the specified replication throughput of the move operation in terms of Kb/s, Mb/s or Gb/s.

**[-actual-duration <timeticks>]** - Duration of Move

If this parameter is specified, the command displays move operations that match the specified duration in days, hours, minutes and seconds for which the volume move was or is in progress.

**[-source-aggregate <aggregate name>]** - Source Aggregate

If this parameter is specified, the command displays move operations that match the specified name of the aggregate where the volume being moved originally resides or resided.

**[-start-time <Date>]** - Start Time of Move

If this parameter is specified, the command displays move operations that match the specified date and time in the cluster time zone when the volume move operation started.

**[-state {healthy|warning|alert|failed|done}]** - Move State

If this parameter is specified, the command displays move operations that match the specified state of the volume move operation.

## Examples

The following example lists status of volume move operation for a volume vol2 on a Vserver vs0

```
cluster1::> volume move show -vserver vs0 -volume vol2
Vserver Name: vs0
Volume Name: vol2
Actual Completion Time: -
Specified Action For Cutover: defer_on_failure
Specified Cutover Attempts: 3
Specified Cutover Time Window: 45
Time Cutover was Triggered: -
Time Cutover was last triggered: -
Destination Aggregate: cluster1_aggr2
Detailed Status: Transferring data: 3.67GB sent.
Estimated Time of Completion: Sat Jul 16 20:25:50 2011
Managing Node: node1
Percentage Complete: 36%
Move Phase: replicating
Estimated Remaining Duration: 00:01
Replication Throughput: 61.08MB/s
Duration of Move: 00:02
Source Aggregate: cluster1_aggr1
Start Time of Move: Sat Jul 16 20:22:01 2011
Move State: healthy
```

The following example lists status of running and failed volume move operations in the cluster.

```
cluster1::> volume move show
Time-To-Complete  Vserver  Volume  State  Move Phase  Percent-Complete
-----
vs0              s1       alert   cutover_hard_deferred
98%
vs0              vol2     failed  failed      -
2 entries were displayed.
```

The following example lists status of all the volume move operations in the cluster.

```
cluster::> vol move show -phase *
(volume move show)
```

Time-To-Complete	Vserver	Volume	State	Move Phase	Percent-Complete	
-----	vs0	s1	alert	cutover_hard	deferred	-
	vs0	s2	done	completed	98%	-
	vs0	vol1	failed	failed	100%	-
	3 entries were displayed.					

Time-To-Complete	Vserver	Volume	State	Move Phase	Percent-Complete	
-----	vs0	vol1	done	completed	100%	-
	vs0	vol2	done	completed	100%	-
	2 entries were displayed.					

---

## volume move start

Start moving a volume from one aggregate to another aggregate

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The volume move start command moves a flexible volume from one storage aggregate to another. The destination aggregate can be located on the same node as the original aggregate or on a different node. The move occurs within the context of the same Vserver.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the volume that will be moved.

**-destination-aggregate** <aggregate name> - Destination Aggregate

This specifies the aggregate to which the volume will be moved.

**[-cutover-window** <integer>] - Cutover time window in seconds

This specifies the time interval to completely cutover operations from the original volume to the moved volume. The default value is 45 seconds. The range for valid input is from 30 to 300 seconds, inclusive.

**[-cutover-attempts** <integer>] - Number of Cutover attempts

This specifies the number of cutover attempts Data ONTAP will make. The default value is 3. The range for valid input is from 1 to 25, inclusive.

**[-cutover-action** {abort\_on\_failure|defer\_on\_failure|force|wait}] - Action for Cutover

Specifies the action to be taken for cutover. Default is "defer\_on\_failure". If "abort\_on\_failure" action is specified, the job will try to cutover until cutover attempts are exhausted. If it fails to cutover, it will cleanup and end the operation. If "defer\_on\_failure" action is specified, the job will try to cutover until the cutover attempts are exhausted. If it fails to cutover, it will move into "cutover deferred" state. This is the default option. The volume move job waits for the user to issue a volume move trigger-cutover command to



---

restart the cutover process. If "force" action is specified, the job will try to cutover until the cutover attempts are exhausted and force the cutover at the expense of disrupting the clients. If "wait" action is specified, when the job hits the decision point, it will not go into cutover automatically, instead it will wait for the user to issue a volume move trigger-cutover command as the signal to try the cutover.

**[-perform-validation-only [true]]** - Performs validation checks only

This is a boolean option allowing the user to perform pre-move validation checks for the intended volume. When set to true, the command only performs the checks without creating a move job. The default value is false.

**[-foreground {true|false}]** - Foreground Process

This specifies whether the volume move operation runs as a foreground process. The default setting is false (that is, the operation runs in the background).

## Examples

The following example performs a validation-check for a volume named `volume_test` on a Vserver named `vs0` to determine if it can be moved to a destination-aggregate named `dest_aggr`.

```
node::> volume move start -vserver vs0 -volume volume_test -destination-aggregate dest_aggr -perform-validation-only true
```

## volume move trigger-cutover

Trigger cutover of a move job

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

## Description

This command causes a deferred volume move job to attempt cutover. Unless the force option is set, cutover entry is not guaranteed.

## Parameters

**-vserver** <vserver name> - Vserver Name

The Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

The volume that will be moved.

---

**[-force [true]]** - Force Cutover

The optional parameter, when set to true, forces cutover without any confirmation and could possibly cause client I/O disruptions. Default is false.

## Examples

```
cluster1::>volume move trigger-cutover -vserver vs0 -volume testvol_1 -force true
```

---

## volume move target-aggr show

List target aggregates compatible for volume move

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The volume move target-aggr show displays information about compatible target aggregates for the specified volume to be moved to.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance ] }

If you specify the -instance parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name (Required field)

This specifies the Vserver on which the volume is located.

[-volume <volume name>] - Volume Name (Required field)

This specifies the volume that will be moved.

[-aggregate <aggregate name>] - Aggregate Name

This specifies the aggregate to which the volume might be moved.

[-availsize {<integer>[KB|MB|GB|TB|PB]] - Available size

This specifies the available size on the aggregate.

[-storagetype <text>] - Storage Type

This specifies the storage type of the aggregate. Examples of storage types are “ATA”, “BSAS”, “FCAL”, “LUN”, “SATA”, “SAS” and “SSD”.

### Examples

---

The following example lists target aggregates compatible for moving a volume vol1 on a Vserver vs1

```
stap-u24::> volume move target-aggr show -vserver vs1 -volume v11
Aggregate Name      Available Size      Storage Type
-----
aggr1               113.5GB             FCAL
aggr2               113.5GB             FCAL
2 entries were displayed.
```

---

## volume qtree create

Create a new qtree

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a qtree in the Vserver and volume you specify. You can create up to 4,994 qtrees per volume. This command is not supported on Infinite Volumes.

You can optionally specify the following attributes when creating a new qtree:

- Security style
- Opportunistic lock mode
- UNIX permissions

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume that will contain the qtree you are creating.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree you are creating.

A qtree name cannot contain a forward slash (/) and must be all ASCII characters. The qtree name cannot be more than 64 characters long.

| **-qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format /vol/<volume name>/<qtree name> can be specified instead of specifying volume and qtree as separate arguments.

[**-security-style** {unix|ntfs|mixed|unified}] - Security Style

This optionally specifies the security style for the qtree, which determines how access to the qtree is controlled. The supported values are unix (for UNIX uid, gid and mode bits), ntfs (for CIFS ACLs), and mixed (for NFS and CIFS access). The unified security style,

---

which applies only to Infinite Volumes, cannot be applied to a qtree. If you do not specify a security style for the qtree, it inherits the security style of its containing volume.

**[-oplock-mode {enable|disable}]** - Oplock Mode

This optionally specifies whether oplocks are enabled for the qtree. If you do not specify a value for this parameter, it inherits the oplock mode of its containing volume.

**[-unix-permissions | -m <unix perm>]** - Unix Permissions

This optionally specifies the UNIX permissions for the qtree when the `-security-style` is set to `unix` or `mixed`. You can specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX `ls` command (for example, `-rwxr-x---`). For information on UNIX permissions, see the UNIX or Linux documentation. If you do not specify UNIX permissions for the qtree, it inherits the UNIX permissions of its containing volume.

## Examples

The following example creates a qtree named `qtree1`. The Vserver name is `vs0` and the volume containing the qtree is named `vol1`. The qtree has a mixed security style. Its other attributes are inherited from volume `vol1`.

```
cluster1::> volume qtree create -vserver vs0 -volume vol1 -qtree qtree1 -
security-style mixed
```

The following example uses a 7G-compatible command to create the qtree.

```
cluster1::> vsserver context vs0
vs0::> qtree create /vol/vol1/qtree1
```

## volume qtree delete

Delete a qtree

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command deletes a qtree. The length of time that it takes to delete a qtree depends on the number of directories and files it contains. You can monitor the progress of the delete operation by using the `job show` and `job watch-progress` commands, respectively. This command is not supported on Infinite Volumes.

The automatically created qtree in the volume - `qtree0`, listed in CLI output as `""` - cannot be deleted.

---

Note:

Quota rules associated with this qtree in all the quota policies will be deleted when you delete this qtree.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume containing the qtree to be deleted.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree to be deleted.

| **-qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format /vol/<volume name>/<qtree name> can be specified instead of specifying volume and qtree as separate arguments.

**[-force** [true]] - Force Delete (privilege: advanced)

This optionally forces the qtree delete operation to proceed when the qtree contains files. The default setting is false (that is, the qtree will not be deleted if it contains files). This parameter is available only at the advanced privilege and higher.

**[-foreground** [true]] - Foreground Process

This optionally specifies whether the qtree delete operation runs as a foreground process. The default setting is false (that is, the operation runs in the background).

## Examples

The following example deletes a qtree named qtree4. The Vserver name is vs0 and the volume containing the qtree is named vol1.

```
cluster1::> volume qtree delete -vserver vs0 -volume vol1 -qtree qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume vol1 vserver vs0?
{y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume vol1 vserver vs0.
```

## See Also

job show   job watch-progress

---

## volume qtree modify

Modify qtree attributes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows you to modify the following attributes of an existing qtree in the given Vserver and volume:

- Security style
- Opportunistic lock mode
- UNIX permissions

This command is not supported by Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume containing the qtree to be modified.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree to be modified. You can modify the attributes of qtree0 (represented as "" in the CLI) by omitting the `-qtree` parameter from the command or by specifying the value "" for the `-qtree` parameter.

| **-qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format `/vol/<volume name>/<qtree name>` can be specified instead of specifying volume and qtree as separate arguments. The automatically created qtree0 can be represented as `/vol/<volume name>`.

[**-security-style** {unix|ntfs|mixed|unified}] - Security Style

This optionally modifies the security style for the qtree. The supported values are `unix` (for UNIX uid, gid and mode bits), `ntfs` (for CIFS ACLs), and `mixed` (for NFS and CIFS access). The unified security style, which applies only to Infinite Volumes, cannot be



---

applied to a qtree. Modifying a qtree's security style will not affect any of the files in the other qtrees of this volume.

**[-oplock-mode {enable|disable}]** - Oplock Mode

This optionally modifies whether oplocks are enabled for the qtree.

Modifying qtree0's oplock mode will not affect any of the files in the other qtrees of this volume.

**[-unix-permissions <unix perm>]** - Unix Permissions

This optionally modifies the UNIX permissions for the qtree. You can specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX ls command (for example, -rwxr-x---). For information on UNIX permissions, see the UNIX or Linux documentation.

The unix permissions can be modified only for qtrees with unix or mixed security style.

## Examples

The following example modifies a qtree named qtree1. The Vserver name is vs0 and the volume containing the qtree is named vol1. The qtree now has a UNIX security style and oplocks are enabled.

```
cluster1::> volume qtree modify -vserver vs0 -volume vol1 -qtree qtree1 -  
security-style unix -oplocks enabled
```

## volume qtree oplocks

Modify qtree oplock mode

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command allows you to display or modify the opportunistic lock mode of a qtree. This command is not supported on Infinite Volumes.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

---

This specifies the name of the volume containing the qtree.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree for which the oplock mode is being displayed or modified.

**| -qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format /vol/<volume name>/<qtree name> can be specified instead of specifying volume and qtree as separate arguments. The automatically created qtree0 can be represented as /vol/<volume name>.

**[-oplock-mode** {enable|disable}] - Oplock Mode

This specifies the new oplock mode of the qtree. If this parameter is not specified, then the current oplock mode of the qtree is displayed.

Modifying qtree0's oplock mode will not affect any of the files in the other qtrees of this volume.

## Examples

The following example displays the oplock mode of a qtree called qtree1. The Vserver name is vs0 and the volume containing the qtree is named vol1.

```
cluster1::> volume qtree oplocks -vserver vs0 -volume vol1 -qtree qtree1
/vol/vol1/qtree1 has mixed security style and oplocks are disabled.
```

The following example modifies the oplock mode of a qtree called qtree2 to enabled. The Vserver name is vs0 and the volume containing the qtree is named vol1.

```
cluster1::> volume qtree oplocks -vserver vs0 -volume vol1 -qtree qtree2 -oplock-
mode enable
```

The following example uses a 7G-compatible command to display and modify the oplock mode of a qtree.

```
cluster1::> vserver context vs0
vs0::> qtree oplocks /vol/vol1/qtree1
/vol/vol1/qtree1 has mixed security style and oplocks are disabled.
vs0::> qtree oplocks /vol/vol1/qtree2 enable
```

---

## volume qtree rename

Rename an existing qtree

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows you to rename an existing qtree. This command is not supported on Infinite Volumes.

The automatically created qtree in the volume - qtree0, listed in CLI output as "" - cannot be renamed.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume containing the qtree to be renamed.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree to be renamed.

| **-qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format /vol/<volume name>/<qtree name> can be specified instead of specifying volume and qtree as separate arguments.

**-newname** <qtree name> - Qtree New Name

This specifies the new name of the qtree. The new qtree name cannot contain a forward slash (/) and cannot be more than 64 characters long.

### Examples

The following example renames a qtree named qtree3 to qtree4. The Vserver name is vs0 and the volume containing the qtree is named vol1.

```
cluster1::> volume qtree rename -vserver vs0 -volume vol1 -qtree qtree3 -newname  
qtree4
```

---

## volume qtree security

Modify qtree security style

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows you to display or modify the security style of a qtree. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

{ **-volume** <volume name> - Volume Name

This specifies the name of the volume containing the qtree.

**-qtree** <qtree name> - Qtree Name

This specifies the name of the qtree for which the security style is being displayed or modified.

| **-qtree-path** <qtree path> } - Qtree Path

The qtree path argument in the format /vol/<volume name>/<qtree name> can be specified instead of specifying volume and qtree as separate arguments. The automatically created qtree0 can be represented as /vol/<volume name>.

[**-security-style** {unix|ntfs|mixed|unified}] - Security Style

This specifies the new security style of the qtree. If this parameter is not specified, then the current security style of the qtree is displayed. The supported values are unix (for UNIX uid, gid and mode bits), ntfs (for CIFS ACLs), and mixed (for NFS and CIFS access). The unified security style, which applies only to Infinite Volumes, cannot be applied to a qtree. Modifying a qtree's security style will not affect any of the files in the other qtrees of this volume.

### Examples

The following example displays the security style of a qtree called qtree1. The Vserver name is vs0 and the volume containing the qtree is named vol1.

---

```
cluster1::> volume qtree security -vserver vs0 -volume voll -qtree qtree1
/vol/voll/qtree1 has mixed security style and oplocks are disabled.
```

The following example modifies the security style of a qtree called qtree2 to unix. The Vserver name is vs0 and the volume containing the qtree is named voll.

```
cluster1::> volume qtree security -vserver vs0 -volume voll -qtree qtree2 -
security-style unix
```

The following example uses a 7G-compatible command to display and modify the security style of a qtree.

```
cluster1::> vserver context vs0
vs0::> qtree security /vol/voll/qtree1
/vol/voll/qtree1 has mixed security style and oplocks are disabled.
vs0::> qtree security /vol/voll/qtree2 unix
```

---

## volume qtree show

Display a list of qtrees

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays information about qtrees for online volumes. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays the following information about all qtrees in the cluster:

- Vserver name
- Volume name
- Qtree name
- Security style (unix, ntfs, mixed or unified)
- Whether oplocks is enabled
- Status (normal, readonly, snapvaulted, or snapmirrored)

The display will also include information about Qtree 0. When you create a volume, a special qtree referred to as "qtree0", also called the default qtree is automatically created for the volume. It represents all of the data stored in a volume that isn't contained in a qtree. In the CLI output, qtree0 is denoted by empty quotation marks ("") and has the ID zero (0). The qtree called qtree0 cannot be manually created or deleted. This command is not supported on Infinite Volumes.

The qtree status indicates readonly for data protection and load sharing volumes. Snapmirrored and Snapvaulted qtrees are not supported.

To display detailed information about a single qtree, run the command with the `-instance` and `-qtree` parameters. The detailed view provides all of the information in the previous list and the following additional information:

- UNIX permissions
- Qtree ID

### Parameters

{ [-fields <fieldname>, ...]

---

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-id]**

If this parameter is specified, the command displays qtree IDs in addition to the default output .

| **[-instance]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays information about the qtrees in the specified Vserver.

{ **[-volume <volume name>]** - Volume Name

If this parameter is specified, the command displays information about the qtrees in the specified volume.

**[-qtree <qtree name>]** - Qtree Name

If this parameter is specified, the command displays information about the qtrees that have the specified name.

| **[-qtree-path <qtree path>]** } - Qtree Path

If this parameter is specified, the command displays information about the qtrees that have the specified path.

**[-security-style {unix|ntfs|mixed|unified}]** - Security Style

If this parameter is specified, the command displays information about the qtrees that have the specified security style. The unified security style, which applies only to Infinite Volumes, cannot be applied to a qtree.

**[-oplock-mode {enable|disable}]** - Oplock Mode

If this parameter is specified, the command displays information about the qtrees that have the specified oplock mode.

**[-unix-permissions | -m <unix perm>]** - Unix Permissions

If this parameter is specified, the command displays information about the qtrees that have the specified UNIX permissions.

**[-qtree-id <integer>]** - Qtree Id

---

If this parameter is specified, the command displays information about the qtrees that have the specified ID. A valid qtree ID is an integer from 0 to 4994. All qtree0 (automatically created) qtrees have an ID of zero (0).

**[-status {normal|readonly|snapvaulted|snapmirrored}] - Qtree Status**

If this parameter is specified, the command displays information about the qtrees that have the specified status.

## Examples

The following example displays default information about all qtrees along with each qtree ID. Note that on vs0, no qtrees have been manually created, so only the automatically created qtrees referred to as qtree 0 are shown. On vs1, the volume named vs1\_vol1 contains qtree 0 and two manually created qtrees, qtree1 and qtree2.

```
cluster1::> volume qtree show -id
Vserver      Volume      Qtree      Style      Oplocks      Status      Id
-----
vs0          vs0_vol1    " "        unix        enable        readonly    0
vs0          vs0_vol2    " "        unix        enable        normal      0
vs0          vs0_vol3    " "        unix        enable        readonly    0
vs0          vs0_vol4    " "        unix        enable        readonly    0
vs0          root_vs_vs0 " "        unix        enable        normal      0
vs1          vs1_vol1    " "        unix        enable        normal      0
vs1          vs1_vol1    qtree1     unix        disable       normal      1
vs1          vs1_vol1    qtree2     unix        enable        normal      2
vs1          root_vs_vs1 " "        unix        enable        normal      0
9 entries were displayed.
```



---

## volume qtree statistics-reset

Reset qtree statistics in a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command resets qtree statistics for all qtrees in a volume. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume containing the qtree belongs.

**-volume** <volume name> - Volume Name

This specifies the name of the volume containing the qtrees whose statistics you want to reset.

### Examples

The following example resets statistics for all qtrees on the the volume named vol1 on the Vserver named vs0.

```
cluster1::> volume qtree statistics-reset -vserver vs0 -volume vol1
```

## volume qtree statistics

Display qtree statistics

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays NFS and CIFS operations statistics for qtrees. Note that qtree statistics are available only when the volume containing the qtree is online. This command is not supported on Infinite Volumes.

---

Statistics are cumulative values from the time the volume is brought online or when the statistics have been reset by using the "volume qtree statistics-reset" command.

The command output depends on the parameters specified with the command. If no parameters are specified, the command displays the following statistics information about all qtrees:

- Vserver name
- Volume name
- Qtree name
- NFS operations
- CIFS operations

Note:

Qtree statistics are not persistent. If you restart a node, if a storage takeover and giveback occurs, or if the containing volume is set to offline and then online, qtree statistics are set to zero.

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**internal** ] (privilege: advanced)

If this parameter is specified, the output will also include the internal operation statistics. Internal operation is any operation on the qtree that originated within Data ONTAP software.

| [-**no-reset** ] (privilege: advanced)

If this parameter is specified, the output will display the NFS and CIFS op statistics since the time the volume was online.

| [-**no-reset-internal** ] (privilege: advanced)

If this parameter is specified, the output will also include the internal op statistics since the time the volume was online.

| [-**instance** ] }

---

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays information about the qtrees on the specified Vserver.

**{ [-volume <volume name>]** - Volume Name

If this parameter is specified, the command displays information about the qtrees on the specified volume.

**[-qtree <qtree name>]** - Qtree Name

If this parameter is specified, the command displays information about the specified qtree.

**| [-qtree-path <qtree path>]** } - Qtree Path

The qtree path argument in the format `/vol/<volume name>/<qtree name>` can be specified instead of specifying volume and qtree as separate arguments. The automatically created qtree0 can be represented as `/vol/<volume name>`.

**[-nfs-ops <Counter64>]** - NFS operations since reset

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of NFS operations since the statistics was zeroed.

**[-cifs-ops <Counter64>]** - CIFS operations since reset

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of CIFS operations since the statistics was zeroed.

**[-internal-ops <Counter64>]** - Internal operations since reset (privilege: advanced)

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of internal operations since the statistics was zeroed.

**[-no-reset-nfs-ops <Counter64>]** - NFS operations since online (privilege: advanced)

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of NFS operations since the volume was online.

**[-no-reset-cifs-ops <Counter64>]** - CIFS operations since online (privilege: advanced)

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of CIFS operations since the volume was online.

**[-no-reset-internal-ops <Counter64>]** - Internal operations since online (privilege: advanced)

If this parameter is specified, the command displays information about qtrees that have the corresponding cumulative number of internal operations since the volume was online.

### Examples

The following example displays statistics information for all qtrees on the Vserver named vs0.

```
cluster1::> volume qtree statistics -vserver vs0
Vserver      Volume      Qtree      NFS Ops      CIFS Ops
-----
vs0          vol0          qtree1      10876         2678
vs0          vol1          qtree1a     16543         0
vs0          vol2          qtree2       0             0
vs0          vol2          qtree2a     0             0
4 entries were displayed.
```

The following example displays statistics information for qtrees on Vserver vs0 that have NFS ops more than 15000.

```
cluster1::> volume qtree statistics -vserver vs0 -nfs-ops >15000
Vserver      Volume      Qtree      NFS Ops      CIFS Ops
-----
vs0          vol1          qtree1a     16543         0
```

### See Also

volume qtree statistics-reset

---

## volume quota modify

Modify quota state for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command allows you to modify the following quota attributes for one or more volumes:

- Quota state
- Whether quota exceeded messages are logged or not
- Frequency with which quota exceeded messages are logged

Modifications to the quota state for a volume creates a job to perform the quota state changes for that volume. You can monitor the progress of the job by using the `job show` and `job watch-progress` commands. This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume whose quota attributes you are modifying is located.

**-volume** <volume name> - Volume Name

This specifies the name of the volume whose quota attributes you are modifying.

**[-state <quota\_state>]** - Quota State

This parameter optionally modifies the quota state to one of the following:

- `off` - This indicates that quotas be deactivated for the specified volume.
- `on` - This indicates that quotas be activated for the specified volume.
- `resize` - This indicates that the quota limits be resized according to the values specified in the quota policy assigned to the Vserver. Note that quotas must be activated first for a volume before a resize operation can be performed.

---

Both quota activation and quota resize operations apply the quota rules configured for the volume within the quota policy that is currently assigned to the Vserver. These quota rules are managed by using the commands in the `volume quota policy rule` menu. Quotas, when activated for a volume, go through an initialization process. As part of the quota initialization all the quota rules are applied to the volume. In addition, a filesystem scanner is started to scan the entire filesystem within the volume to bring the quota accounting and reporting up to date. The quota job finishes after the filesystem scanner is started on the volume. The quota state for the volume is `initializing` until the filesystem scanner finishes scanning the entire filesystem. After the scanning is complete, the quota state will be `on`.

When quotas are resized, the quota state is `resizing` until the resizing operation finishes. As part of this operation, the quota limits for quotas currently in effect are resized to the limits currently configured for the volume. After the quota resize operation finishes, the quota state will be `on`.

Quota state changes can also be performed using the commands `volume quota on`, `volume quota off` and `volume quota resize`.

#### **[-logging {on|off}] - Logging Messages**

This parameter optionally specifies whether quota exceeded syslog/EMS messages are logged in the system log messages. When it is set to `on`, quota exceeded messages are generated when the user exceeds the quota's disk limit or the file limit through a NFS/CIFS operation or any operation within the Data ONTAP software. When set to `off` no quota exceeded messages are generated. This parameter can be changed only after quotas are activated for a volume.

#### **[-logging-interval <text>] - Logging Interval**

This parameter optionally specifies a logging interval, which indicates the frequency with which quota exceeded messages are generated. You can specify a logging interval in the `<integer><suffix>` format, where suffix can be minutes (`m`), hours (`h`), or days (`d`), but not combinations thereof (in other words, `90m` is a valid logging interval, but `1h30m` is not a valid logging interval). You can modify the logging interval only when the logging is `on`. When quotas are first activated, the logging parameter is automatically set to `on`, and the logging interval set to `1h`. If continuous logging is required, an interval of `0m` should be specified. This parameter can be changed only after quotas are activated for a volume.

Note:

quota message logging may not occur at exactly the same interval rate as specified by the user, especially for very small intervals. This is due to the behavior of the logging system that buffers messages instead of outputting them immediately. Setting the

---

logging interval to 0m can cause lots of quota exceeded messages to be logged in the system log messages.

### **[-foreground [true]] - Foreground Process**

This parameter optionally specifies whether the job created by quota state modify operation runs as a foreground process. The default setting is `false` (that is, the quota state modify operation runs in the background). When set to `true`, the command will not return until the job completes.

## **Examples**

The following example activates quotas on the volume named `vol1`, which exists on Vserver `vs0`.

```
cluster1::> volume quota modify -vserver vs0 -volume vol1 -state on
[Job 24] Job is queued: Quota ON Operation on vserver vs0 volume vol1.
```

The following example turns on quota message logging and sets the logging interval to 4 hours.

```
cluster1::> volume quota modify -vserver vs0 -volume vol1 -logging on -logging-
interval 4h
```

The following example resizes quota limits on a volume.

```
cluster1::> volume quota modify -vserver vs0 -volume vol1 -state resize -
foreground true
[Job 80] Job succeeded: Successful
```

## **See Also**

`volume quota policy rule` `volume quota on` `volume quota off` `volume quota resize`  
`job show` `job watch-progress` `volume quota show`

---

## volume quota off

Turn off quotas for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a job to deactivate quotas for the specified volume. This command is not supported on Infinite Volumes. You can monitor the progress of the job by using the `job show` and `job watch-progress` commands.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the name of the volume on which you are deactivating quotas.

**[-foreground [true]]** - Foreground Process

This optionally specifies whether the job created for deactivating quotas runs as a foreground process. The default setting is `false` (that is, the operation runs in the background). When set to `true`, the command will not return until the job completes.

### Examples

The following example deactivates quotas on the volume named `vol1`, which exists on Vserver `vs0`.

```
cluster1::> volume quota off -vserver vs0 -volume vol1
[Job 23] Job is queued: Quota OFF Operation on vserver vs0 volume vol1.
```

The following example uses a 7G-compatible command to deactivate quotas on the volume named `vol1` which exists on Vserver `vs0`.

```
cluster1::> vserver context vs0
vs0::> quota off vol1
[Job 25] Job is queued: Quota OFF Operation on vserver vs0 volume vol1.
```

### See Also

`job show` `job watch-progress` `volume quota modify`



---

## volume quota on

Turn on quotas for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a job to activate quotas for the specified volume. This command is not supported on Infinite Volumes. You can monitor the progress of the job by using the `job show` and `job watch-progress` commands.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the name of the volume on which you are activating quotas.

**[-foreground | -w [true]]** - Foreground Process

This optionally specifies whether the job created for activating quotas runs as a foreground process. The default setting is `false` (that is, the operation runs in the background). When set to `true`, the command will not return until the job completes. The quota job finishes after the filesystem scanner is started. The quota state for the volume is `initializing` until the filesystem scanner finishes scanning the entire filesystem. After the scanning is complete, the quota state will be `on`.

### Examples

The following example activates quotas on the volume named `vol1`, which exists on Vserver `vs0`.

```
cluster1::> volume quota on -vserver vs0 -volume vol1
[Job 23] Job is queued: Quota ON Operation on vserver vs0 volume vol1.
```

The following example uses a 7G-compatible command to activate quotas on the volume named `vol1` which exists on Vserver `vs0`.

```
cluster1::> vserver context vs0
vs0::> quota on -w vol1
[Job 25] Job is queued: Quota ON Operation on vserver vs0 volume vol1.
[Job 25] Job succeeded: Successful
```

---

## See Also

job show   job watch-progress   volume quota modify

---

## volume quota report

Display the quota report for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the quota report for all volumes in each Vserver that are online and for which quotas are activated. Quota report includes the quota rules (default, explicit, and derived) in effect and the associated resource usage (disk space and files). If quotas are still initializing for a specific volume, that volume is not included. This command is not supported on Infinite Volumes.

This command displays the following information:

- Vserver name
- Volume name
- Index - This is a unique number within a volume assigned to each quota rule displayed in the quota report.
- Tree name - This field gives the name of the qtree if the quota rule is at the qtree level. It is empty if the quota rule is at the volume level.
- Quota type - Type of quota rule (*tree* or *user* or *group*).
- Quota target - This field gives the name of the target of the quota rule. For tree quota rules, it will be the qtree ID of the qtree. For user quota rules, it will be the UNIX user name or the Windows user name. For group quota rules, it will be the UNIX group name. For default rules (*tree* or *user* or *group*), this will display " \* ". If the UNIX user identifier, UNIX group identifier, or Windows security identifier no longer exists or if the identifier-to-name conversion fails, the target appears in numeric form.
- Quota target ID - This field gives the target of the quota rule in numeric form. For tree quota rules, it will be the qtree ID of the qtree. For group quota rules, it will be the UNIX group identifier. For UNIX user quota rules, it will be the UNIX user identifier. For Windows user quota rules, it will be the Windows security identifier in its native format. For default rules (*tree* or *user* or *group*), " \* " will be displayed.
- Disk space used - For a default quota, the value is 0.
- Disk space limit

- Soft disk space limit
- Threshold for disk space limit
- Files used - For a default quota, the value is 0.
- File limit
- Soft file limit
- Quota specifier - For an explicit quota, this field shows how the quota target was configured by the administrator using the volume quota policy rule command. For a default quota, the field shows " \* ". For a derived tree quota, this field shows the qtree path. For a derived user and group quota, the field is either blank or " \* ".

The following parameters: `-soft`, `-soft-limit-thresholds`, `-target-id`, `-thresholds`, `-fields` and `-instance` display different set of fields listed above. For example, `-soft` will display the soft disk space limit and soft file limit apart from other information. Similarly `-target-id` will display the target in the numeric form.

A quota report is a resource intensive operation. If you run it on many volumes in the cluster, it might take a long time to complete. A more efficient way would be to view the quota report for a particular volume in a Vserver.

Depending upon the quota rules configured for a volume, the quota report for a single volume can be large. If you want to monitor the quota report entry for a particular tree/user/group repeatedly, find the index of that quota report entry and use the `-index` field to view only that quota report entry. See the examples section for an illustration.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-soft ]**

If this parameter is specified, the command display will include the soft disk space limit and the soft file limit.

| **[-soft-limit-thresholds ]**

If this parameter is specified, the command display will include the soft disk space limit, threshold for disk space limit and soft file limit.

| **[-target-id ]**

---

If this parameter is specified, the command will display the target of a user or group quota rule in numeric form.

| **[-thresholds ]**

If this parameter is specified, the command display will include the threshold for disk space limit.

| **[-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays the quota report for volumes in the specified Vserver.

**[-volume <volume name>]** - Volume Name

If this parameter is specified, the command displays the quota report for the specified volume.

**[-index <integer>]** - Index

If this parameter is specified, the command displays the quota report for the quota rules that have the specified index.

**[-tree <qtree name>]** - Qtree Name

If this parameter is specified, the command displays the quota report for the quota rules that have the specified qtree name.

**[-quota-type <text>]** - Quota Type

If this parameter is specified, the command displays the quota report for the quota rules of the given type.

**[-quota-target <text>]** - Quota Target

If this parameter is specified, the command displays the quota report for the quota rules that have the specified quota target.

**[-quota-target-id <text>]** - Quota Target ID

If this parameter is specified, the command displays the quota report for the quota rules that have the specified quota target identifier.

**[-disk-used {<integer>[KB|MB|GB|TB|PB]}]** - Disk Space Used

If this parameter is specified, the command displays the quota report for the quota rules that have the specified disk space used value.

---

**[-disk-limit {<integer>[KB|MB|GB|TB|PB]]** - Disk Space Limit

If this parameter is specified, the command displays the quota report for the quota rules that have the specified disk space limit.

**[-files-used <integer>]** - Files Used

If this parameter is specified, the command displays the quota report for the quota rules that have the specified files used value.

**[-file-limit <integer>]** - Files Limit

If this parameter is specified, the command displays the quota report for the quota rules that have the specified file limit.

**[-threshold {<integer>[KB|MB|GB|TB|PB]]** - Disk Space Threshold

If this parameter is specified, the command displays the quota report for the quota rules that have the specified threshold for disk space limit.

**[-soft-disk-limit {<integer>[KB|MB|GB|TB|PB]]** - Soft Disk Space Limit

If this parameter is specified, the command displays the quota report for the quota rules that have the specified soft disk space limit.

**[-soft-file-limit <integer>]** - Soft Files Limit

If this parameter is specified, the command displays the quota report for the quota rules that have the specified soft file limit.

**[-quota-specifier <text>]** - Quota Specifier

If this parameter is specified, the command displays the quota report for the quota rules that have the specified quota specifier.

**[-path <text>]** - Path

If this parameter is specified, the command will display the quota report for the quota rules that are applicable for the file in the specified path. The format of the path to the file should begin with /vol/<volume name>/. The quota rules that are applicable typically consists of the tree quota rule corresponding to the qtree in which the file resides within the volume, user quota rule at the volume and qtree level corresponding to the UNIX user identifier or the Windows security identifier associated with the file and the group quota rule at the volume and qtree level corresponding to the UNIX group identifier associated with the file.

## Examples

The following example displays the quota report for all the volumes.

```
cluster1::> volume quota report
Vserver: vs0
```

Volume	Tree	Type	ID	-----Disk----- Used Limit	-----Files----- Used Limit	Quota Specifier
vol2		tree	*	0.00B 100MB	0 10000	*
vol2	vxw02	tree	3	0.00B 200MB	1 20000	vxw02
vol2		user	*	0.00B 50MB	0 -	*
vol2	vxw02	user	Sam, Engr\Sammy	0.00B 100MB	0 -	Sam
vol2		group	*	0.00B 500MB	0 -	*
vol2	q1	tree	1	1MB 100MB	2 10000	q1
vol2	q1	user	*	0.00B 50MB	0 -	
vol2	q1	group	*	0.00B 500MB	0 -	
vol2	q1	group	root	1MB -	2 -	
vol2	vxw01	tree	2	0.00B 100MB	1 10000	vxw01
vol2	vxw01	user	*	0.00B 50MB	0 -	
vol2	vxw01	group	*	0.00B 500MB	0 -	
vol2	vxw01	group	root	0.00B -	1 -	
vol2	vxw02	user	*	0.00B 50MB	0 -	
vol2	vxw02	group	*	0.00B 500MB	0 -	
vol2	vxw02	group	root	0.00B -	1 -	
vol2	vxw03	tree	4	0.00B 100MB	1 10000	vxw03
vol2	vxw03	user	*	0.00B 50MB	0 -	
vol2	vxw03	group	*	0.00B 500MB	0 -	
vol2	vxw03	group	root	0.00B -	1 -	
vol2		group	root	1MB -	6 -	
vol2	q1	user	root, Engr\root	0.00B -	1 -	
vol2	vxw01	user	root, Engr\root	0.00B -	1 -	
vol2	vxw02	user	root, Engr\root	0.00B -	1 -	
vol2	vxw03	user	root, Engr\root	0.00B -	1 -	
vol2		user	root, Engr\root	0.00B -	5 -	
vol2		user	john, Engr\John	1MB 50MB	1 -	*
vol2	q1	user	john, Engr\John	1MB 50MB	1 -	

28 entries were displayed.

The following example displays the quota report for the quota rules that are applicable for the given path to a file.

```
cluster1::> volume quota report -path /vol/vol2/q1/file1
Vserver: vs0
```

Volume	Tree	Type	ID	-----Disk----- Used Limit	-----Files----- Used Limit	Quota Specifier
vol2	q1	tree	1	1MB 100MB	2 10000	q1
vol2	q1	group	root	1MB -	2 -	
vol2		group	root	1MB -	6 -	
vol2		user	john, Engr\John	1MB 50MB	1 -	*
vol2	q1	user	john, Engr\John	1MB 50MB	1 -	

5 entries were displayed.

The following example displays the quota report with the target in the numeric form for the given path to a file.

```
cluster1::> volume quota report -path /vol/vol2/q1/file1 -target-id
Vserver: vs0
```

Volume	Tree	Type	ID	-----Disk----- Used Limit	-----Files----- Used Limit	Quota Specifier
vol2	q1	tree	1	1MB 100MB	2 10000	q1
vol2	q1	group	0	1MB -	2 -	
vol2		group	0	1MB -	6 -	
vol2		user	8017,S-1-5-21-3567637-1906459281-1427260136-60871	1MB 50MB	1 -	*

---

```
vol2      ql      user      8017,S-1-5-21-3567637-1906459281-1427260136-60871
                                     1MB      50MB      1      _
5 entries were displayed.
```

The following example shows how to monitor the quota report for a particular user/tree/group. First, the quota report command is issued with `-instance` to see the index field for the quota report entry we are interested in. Next, the quota report is issued with the `-index` field specified to fetch only that particular quota report entry repeatedly to view the usage over time.

```
cluster1::> volume quota report -vserver vs0 -volume voll1 -quota-type user -
quota-target john -tree ql -instance
```

```
Vserver Name: vs0
Volume Name: voll1
Index: 10
Qtree Name: ql
Quota Type: user
Quota Target: john
Quota Target ID: 5433
Disk Space Used: 50.5MB
Disk Space Limit: 100MB
Files Used: 205
Files Limit: -
Disk Space Threshold: 95MB
Soft Disk Space Limit: 80MB
Soft Files Limit: -
Quota Specifier: john
```

```
cluster1::> volume quota report -vserver vs0 -volume voll1 -index 10
```

```
Vserver Name: vs0
Volume Name: voll1
Index: 10
Qtree Name: ql
Quota Type: user
Quota Target: john
Quota Target ID: 5433
Disk Space Used: 55MB
Disk Space Limit: 100MB
Files Used: 410
Files Limit: -
Disk Space Threshold: 95MB
Soft Disk Space Limit: 80MB
Soft Files Limit: -
Quota Specifier: john
```

```
cluster1::> volume quota report -vserver vs0 -volume voll1 -index 10
```

```
Vserver Name: vs0
Volume Name: voll1
Index: 10
Qtree Name: ql
Quota Type: user
Quota Target: john
Quota Target ID: 5433
Disk Space Used: 60.7B
Disk Space Limit: 100MB
Files Used: 500
Files Limit: -
Disk Space Threshold: 95MB
Soft Disk Space Limit: 80MB
Soft Files Limit: -
Quota Specifier: john
```

## See Also

`volume quota show` `volume quota modify` `volume quota policy rule`



---

## volume quota resize

Resize quotas for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command resizes the quota limits for the quotas currently in effect for the specified volume. It creates a job to resize quotas. This command is not supported on Infinite Volumes. You can monitor the progress of the job by using the `job show` and `job watch-progress` commands.

Note:

Quotas must be activated before quota limits can be resized.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the name of the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the name of the volume on which you are resizing the quota limits and threshold.

**[-foreground** [true]] - Foreground Process

This optionally specifies whether the job created for resizing quotas runs as a foreground process. The default setting is `false` (that is, the operation runs in the background). When set to `true`, the command will not return until the job completes.

### Examples

The following example resizes quotas on the volume named `vol1`, which exists on Vserver `vs0`.

```
cluster1::> volume quota resize -vserver vs0 -volume vol1
[Job 34] Job is queued: Quota RESIZE Operation on vserver vs0 volume vol1.
```

The following example uses a 7G-compatible command to resize quotas on the volume named `vol1` which exists on Vserver `vs0`.

---

```
cluster1::> vserver context vs0
vs0::> quota resize voll
[Job 35] Job is queued: Quota RESIZE Operation on vserver vs0 volume voll.
```

## See Also

[job show](#) [job watch-progress](#) [volume quota modify](#)

---

## volume quota show

Display quota state for volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays information about quotas for online volumes. The command output depends on the parameters specified with the command. Quotas can only be administered on FlexVol volumes. This command is not supported on Infinite Volumes. If no parameters are specified, the command displays the following information for all volumes:

- Vserver name
- Volume name
- Quota state - quota state for this volume. The possible values are as follows:
  - `off` - this state indicates that quotas are deactivated for the volume.
  - `on` - this state indicates that quotas are activated for the volume.
  - `initializing` - this state indicates that quotas are being initialized for the volume.
  - `resizing` - this state indicates that quota limits are being resized for the volume.
  - `corrupt` - this state indicates that quotas are corrupt for this volume.
- Scan status - percentage of the files in the volume scanned by the quota scanner that runs as part of activating quotas.
- Last error - most recently generated error message as part of the last quota operation (`on` or `resize`). Present only if an error has been generated.

To display detailed information about all volumes, run the command with the `-instance` parameter. The detailed view provides all of the information in the previous list and the following additional information:

- Logging messages - whether quota exceeded syslog/EMS messages are logged or not. For volumes where the quota logging parameter is set to `on`, quota exceeded messages are generated when a NFS/CIFS operation or any internal

---

Data ONTAP operation is being prevented because the quota disk usage is exceeding the disk limit or the quota file usage is exceeding the file limit. For quotas where the logging parameter is set to `off`, no quota exceeded messages are generated.

- Logging interval - frequency with which quota exceeded messages are logged. This parameter only applies to volumes that have the logging parameter set to `on`.
- Sub status - additional status about quotas for this volume. Following are the possible values reported:
  - `upgrading` - this indicates that the quota metadata format is being upgraded from an older version to a newer version for the volume.
  - `setup` - this indicates that the quotas are being setup on the volume.
  - `transferring rules` - this indicates that the quota rules are being transferred to the volume.
  - `scanning` - this indicates that the quota filesystem scanner is currently running on the volume.
  - `finishing` - this indicates that the quota `on` or `resize` operation is in the final stage of the operation.
  - `done` - this indicates that the quota operation is finished.
  - `none` - this indicates that there is no additional status.
- All errors - collection of all the error messages generated as part of the last quota operation (`on` or `resize`) since the volume was online.
- User quota enforced (advanced privilege only) - indicates whether there are user quota rules being enforced.
- Group quota enforced (advanced privilege only)- indicates whether there are group quota rules being enforced.
- Tree quota enforced (advanced privilege only) - indicates whether there are tree quota rules being enforced.

## Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

---

| **[-logmsg]**

If this parameter is specified, the command displays whether quota exceeded messages are logged and the logging interval for the quota messages.

| **[-instance]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays information for the volumes in the specified Vserver.

**[-volume <volume name>]** - Volume Name

If this parameter is specified, the command displays information for the specified volume.

**[-state <quota\_state>]** - Quota State

If this parameter is specified, the command displays information for the volumes that have the specified quota state.

**[-scan-status <percent>]** - Scan Status

If this parameter is specified, the command displays information about the volumes whose scan-status matches the specified percentage value. The scan status is displayed in the format [0-100]%.

**[-logging {on|off}]** - Logging Messages

If this parameter is specified, the command displays information about the volumes that have the specified logging setting.

**[-logging-interval <text>]** - Logging Interval

If this parameter is specified, the command displays information about the volumes that have the specified quota logging interval.

**[-sub-status <text>]** - Sub Quota Status

If this parameter is specified, the command displays information about the volumes that have the specified quota sub-status.

**[-last-error <text>]** - Last Quota Error Message

If this parameter is specified, the command displays information about the volumes whose last error matches the specified error message.

**[-errors <text>]** - Collection of Quota Errors

---

If this parameter is specified, the command displays information about the volumes whose collection of errors match the specified error message.

**[-is-user-quota-enforced {true|false}]** - User Quota enforced (privilege: advanced)

If this parameter is specified, the command displays information about the volumes that have the specified value for this field.

**[-is-group-quota-enforced {true|false}]** - Group Quota enforced (privilege: advanced)

If this parameter is specified, the command displays information about the volumes that have the specified value for this field.

**[-is-tree-quota-enforced {true|false}]** - Tree Quota enforced (privilege: advanced)

If this parameter is specified, the command displays information about the volumes that have the specified value for this field.

## Examples

The following example displays information about all volumes on the Vserver named vs0.

```
cluster1::> volume quota show -vserver vs0
Vserver   Volume      State      Scan
-----
vs0       root_vs0    off        -
vs0       voll        off        -
          Last_Error: Volume voll has no valid quota rules
vs0       vol2        on         -
vs0       vol3        initializing 30%
4 entries were displayed.
```

The following example displays the logging information for all the volumes.

```
cluster1::volume quota> show -logmsg
Vserver   Volume      State      Logging
-----
vs0       root_vs0    off        -
vs0       voll        off        -
vs0       vol2        on         1h
vs0       vol3        on         1h
4 entries were displayed.
```

The following example displays detailed information in advanced privilege for a volume voll, which exists on Vserver vs0

```
cluster1> set advanced
Warning: These advanced commands are potentially dangerous; use them only when
directed to do so by NetApp personnel.
Do you want to continue? {Y|N}: y
cluster1:*> volume quota show -instance -vserver vs0 -volume voll
          Vserver Name: vs0
          Volume Name: voll
          Quota State: on
          Scan Status: -
```

---

```
      Logging Messages: on
      Logging Interval: 1h
      Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
      User Quota enforced: true
      Group Quota enforced: false
      Tree Quota enforced: false
```

The following example displays the detailed information when quotas are upgrading for volume `vol1`, which exists on Vserver `vs0`.

```
cluster1::*> volume quota show -instance -vserver vs0 -volume vol1

      Vserver Name: vs0
      Volume Name: vol1
      Quota State: initializing
      Scan Status: 3%
      Logging Messages: -
      Logging Interval: -
      Sub Quota Status: upgrading
Last Quota Error Message: -
Collection of Quota Errors: -
      User Quota enforced: -
      Group Quota enforced: -
      Tree Quota enforced: -
```

The following example displays the "Last Quota Error Message" and the "Collection of Quota Errors" for volume `vol1`, which exists on Vserver `vs0`

```
cluster1::> volume quota show -instance -vserver vs0 -volume vol1

      Vserver Name: vs0
      Volume Name: vol1
      Quota State: on
      Scan Status: -
      Logging Messages: on
      Logging Interval: 1h
      Sub Quota Status: none
Last Quota Error Message: second definition for user2 (type:user
target:user2,user4 qtree:"").
Collection of Quota Errors: second definition for user1 (type:user
target:user1,user3 qtree:"").
                        second definition for user2 (type:user
target:user2,user4 qtree:"").
```

---

## volume quota policy copy

Copy a quota policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command copies a quota policy and the rules it contains. This command is not supported on Infinite Volumes. You must enter the following information to copy a quota policy:

- Vserver name
- Policy name
- New policy name

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you are copying the quota policy.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy you are copying.

**-new-policy-name** <text> - New Policy Name

This parameter specifies the name of the new quota policy you are copying to. The new name cannot have more than 32 characters.

### Examples

The following example copies a quota policy named `quota_policy_0` on Vserver `vs0`. It is copied to `quota_policy_1`.

```
cluster1::> volume quota_policy copy -vserver vs0 -policy-name quota_policy_0 -  
new-policy-name quota_policy_1
```

## volume quota policy create

Create a quota policy



---

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

A quota policy is collection of quota rules for all the volumes in a specific Vserver. This command creates a quota policy for a specific Vserver. Multiple quota policies can be created for a Vserver, but only one of them can be assigned to the Vserver. A Vserver can have a maximum of five quota policies. If five quota policies already exist, the command fails and a quota policy must be deleted before another quota policy can be created. This command is not supported on Infinite Volumes.

When you turn on quotas for a volume, the quota rules to be enforced on that volume will be picked from the quota policy that is assigned to the Vserver containing that volume. The quota policy for clustered volumes is equivalent to the `/etc/quotas` file in 7G.

You must enter the following information to create a quota policy:

- Vserver name
- Policy name

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which you are creating the quota policy. You can create a quota policy only for a data Vserver. Quota policies cannot be created for a node or admin Vserver.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy you are creating. The quota policy name cannot be more than 32 characters long and must be unique within the Vserver.

## Examples

The following example creates a quota policy named `quota_policy_0` on Vserver `vs0`.

```
cluster1::> volume quota policy create -vserver vs0 -policy-name quota_policy_0
```

## volume quota policy delete

Delete a quota policy

---

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command deletes a quota policy and all the rules it contains. The policy can be deleted only when it is not assigned to the Vserver. This command is not supported on Infinite Volumes. You must enter the following information to delete a quota policy:

- Vserver name
- Policy name

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver containing the quota policy you want to delete.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy you want to delete.

## Examples

The following example deletes a quota policy named `quota_policy_5` on Vserver `vs0`.

```
cluster1::> volume quota policy delete -vserver vs0 -policy-name quota_policy_5
```

## volume quota policy rename

Rename a quota policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command renames a quota policy. This command is not supported on Infinite Volumes. You must enter the following information to rename a quota policy:

- Vserver name
- Policy name
- New policy name

---

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver containing the quota policy you want to rename.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy you are renaming.

**-new-policy-name** <text> - New Policy Name

This parameter specifies the new name of the quota policy. The new name cannot be more than 32 characters long.

## Examples

The following example renames a quota policy named `quota_policy_0` on Vserver `vs0`. The policy's new name is `quota_policy_1`.

```
cluster1::> volume quota_policy rename -vserver vs0 -policy-name quota_policy_0 -  
new-policy-name quota_policy_1
```

## volume quota policy show

Display the quota policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command displays information about quota policies. This command is not supported on Infinite Volumes. The command displays the following information about all quota policies:

- Vserver name
- Policy name
- When the policy was last modified

## Parameters

{ **[-fields** <fieldname>, ...]

---

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If this parameter is specified, the command displays information about the quota policies for the specified Vserver.

**[-policy-name <text>]** - Policy Name

If this optional parameter is specified, the command displays information about quota policies that match the specified name.

**[-last-modified <MM/DD/YYYY HH:MM:SS>]** - Last Modified

If this optional parameter is specified, the command displays information about quota policies with the last modified time that match the given time.

## Examples

The following example displays information about all quota policies.

```
cluster1::> volume quota policy show
Vserver      Policy Name      Last Modified
-----
vs0           quota_policy_vs0  10/16/2008 17:40:05
vs1           quota_policy_vs1  10/16/2008 17:47:45
vs2           quota_policy_vs2  10/16/2008 17:44:13
vs3           quota_policy_vs3  10/16/2008 17:44:13
4 entries were displayed.
```

---

## volume quota policy rule create

Create a new quota rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a quota policy rule. This command is not supported on Infinite Volumes. You must enter the following information to create a quota policy rule:

- Vserver name
- Quota policy name
- Volume name
- Quota target type
- Target to which the rule applies
- Qtree to which the rule applies

You can optionally specify the following additional attributes for the quota policy rule:

- User mapping
- Hard disk limit
- Hard file limit
- Threshold for disk limit
- Soft disk limit
- Soft file limit

Note:

For a new quota policy rule to get enforced on the volume, you should create the rule in the quota policy assigned to the Vserver. Additionally, a quota off and on or a quota resize operation must be done using the "volume quota modify" command.

### Parameters

**-vserver** <vserver name> - Vserver

---

This parameter specifies the Vserver containing the quota policy for which you are creating a rule.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy in which you are creating a rule.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume for which you are creating a rule.

**-type** {tree|user|group} - Type

This parameter specifies the quota target type of the rule you are creating.

**-target** <text> - Target

This parameter specifies the target to which the quota policy rule applies. For default quota rules, this parameter should be specified as "". For explicit tree quotas rules, this parameter should indicate the qtree name. For explicit user quota rules, this parameter can contain UNIX user name, UNIX user identifier, Windows user name, Windows Security Identifier or a path to an existing object within the volume. If a name contains a space, enclose the entire value in quotes. A UNIX user name cannot include a backslash (\) or an @ sign; user names with these characters are treated as Windows names. For multi-user quotas, this parameter can contain multiple user targets separated by a comma. For explicit group quota rules, this parameter can contain UNIX group name or UNIX group identifier or a path to an existing object within the volume. When a path is specified as the target, it should be of the format /vol/<vol-name>/<path to file from volume root> where the volume matches that of the `-volume` parameter.

**-qtree** <qtree name> - Qtree Name

This parameter specifies the name of the qtree to which the quota rule applies. This parameter is not applicable for tree type rules. For user or group type rules at the volume level, this parameter should contain "".

**[-user-mapping** {on|off}] - User Mapping

This parameter optionally specifies if user mapping needs to be performed for a user quota rule. If this parameter is "on", the UNIX user name specified as the quota target will be mapped to the corresponding Windows user name or vice-versa and quota accounting will be performed for the users together. The mapping will be obtained as configured in "vserver name-mapping".

Note that this parameter can be specified only for quota policy rules of type user. A value of "on" can be specified for this parameter only if the quota target is a UNIX user name or a Windows user name and cannot be specified for multi-user quota targets.

**[-disk-limit** {<size>|-}] - Disk Limit

---

This parameter optionally specifies a hard limit for the disk space that can be consumed by the quota target. The default unit for the disk limit is assumed to be Kilobytes if no units are specified. When the hard disk space limit is reached, no additional disk space can be consumed by the specified target. The value that you specify for this parameter should be greater than or equal to the threshold and soft disk limit. A disk limit of unlimited can be specified with a "-" for this parameter or by not specifying this parameter and will be indicated by a "-". The maximum value is 1,125,899,906,842,620 KB, which is approximately 1,023 PB. The value should be a multiple of 4 KB. If it is not, this field can appear incorrect in quota reports. This happens because the field is always rounded up to the nearest multiple of 4 KB to match disk space limits, which are translated into 4-KB disk blocks. The value can be larger than the amount of disk space available in the volume.

**[-file-limit {<integer>|-}]** - Files Limit

This parameter optionally specifies a hard limit for the number of files permitted on the quota target. When the hard number of files limit is reached, no additional files can be created by the specified target. The value that you specify for this parameter should be greater than or equal to the soft file limit. A file limit of unlimited can be specified with a "-" for this parameter or by not specifying this parameter and will be indicated by a "-". The maximum value is 4,294,967,295.

**[-threshold {<size>|-}]** - Threshold for Disk Limit

This parameter optionally specifies the disk limit threshold for the quota target. The default unit for the disk limit threshold is assumed to be Kilobytes if no units are specified. When the disk limit threshold is exceeded, a console message, an EMS event, and an SNMP trap are generated. The value that you specify for this parameter should be greater than or equal to the soft disk limit and equal to or less than the disk limit. A threshold of unlimited can be specified with a "-" for this parameter or by not specifying this parameter and will be indicated by a "-". The maximum value is 1,125,899,906,842,620 KB, which is approximately 1,023 PB. The value should be a multiple of 4 KB. If it is not, this field can appear incorrect in quota reports. This happens because the field is always rounded up to the nearest multiple of 4 KB to match disk space limits, which are translated into 4-KB disk blocks.

**[-soft-disk-limit {<size>|-}]** - Soft Disk Limit

This parameter optionally specifies a soft limit for the disk space that can be consumed by the quota target. The soft disk limit indicates that the hard limit for the disk space will soon be exceeded. The default unit for the soft disk limit is assumed to be Kilobytes if no units are specified. When the soft limit for the disk space is exceeded, a console message, an EMS event and an SNMP trap are generated. The same happens when the disk space used goes below the specified limit. The value that you specify for this parameter should be equal to or less than the threshold and the disk limit. A soft disk limit of unlimited can be specified with a "-" for this parameter or by not specifying this

---

parameter and will be indicated by a "-". The maximum value is 1,125,899,906,842,620 KB, which is approximately 1,023 PB. The value should be a multiple of 4 KB. If it is not, this field can appear incorrect in quota reports. This happens because the field is always rounded up to the nearest multiple of 4 KB to match disk space limits, which are translated into 4-KB disk blocks.

### **[-soft-file-limit {<integer>|-}] - Soft Files Limit**

This parameter optionally specifies a soft limit for the number of files permitted on the quota target. The soft file limit indicates that the hard limit for the number of files will soon be exceeded. When the soft limit for the number of files is exceeded, a console message, an EMS event and an SNMP trap are generated. The same happens when the files used goes below the specified limit. The value that you specify for this parameter should be equal to or less than the file limit. A soft file limit of unlimited can be specified with a "-" for this parameter or by not specifying this parameter and will be indicated by a "-". The maximum value is 4,294,967,295.

## **Examples**

The following example creates a default tree quota rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to all qtrees on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0
-policy-name quota_policy_0 -volume vol0 -type user -target ""
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the UNIX user myuser for a qtree named qtree1 on volume vol0 with a disk limit of 20 Gigabytes, soft disk limit of 15.4 Gigabytes and threshold limit of 15.4 Gigabytes. User mapping is turned on for this rule.

```
cluster1::> volume quota policy rule create -vserver vs0
-policy-name quota_policy_0 -volume vol0 -type user -target myuser
-qtree qtree1 -user-mapping on -disk-limit 20GB -soft-disk-limit 15.4GB
-threshold 15.4GB
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the Windows user DOMXYZ\myuser for a qtree named qtree1 on volume vol0 with a file limit of 40000 and a soft file limit of 26500. User mapping is turned on for this rule.

```
cluster1::> volume quota policy rule create -vserver vs0
-policy-name quota_policy_0 -volume vol0 -type user -target DOMXYZ\myuser
-qtree qtree1 -user-mapping on -file-limit 40000 -soft-file-limit 26500
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the UNIX user identifier 12345 for a qtree named qtree1 on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0
```



---

```
-policy-name quota_policy_0 -volume vol0 -type user -target 12345  
-qtree qtree1
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the Windows Security Identifier S-123-456-789 for a qtree named qtree1 on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0  
-policy-name quota_policy_0 -volume vol0 -type user  
-target S-123-456-789 -qtree qtree1
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the UNIX group engr for a qtree named qtree1 on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0  
-policy-name quota_policy_0 -volume vol0 -type group -target engr  
-qtree qtree1
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the user who is the owner of the file /vol/vol0/qtree1/file1.txt for qtree qtree1 on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name  
quota_policy_0 -volume vol0 -type user -target /vol/vol0/qtree1/file1.txt  
-qtree qtree1
```

The following example creates a quota policy rule for volume vol0 in Vserver vs0 and in the quota policy named quota\_policy\_0. This quota policy applies to the users specified in the target for qtree qtree1 on volume vol0.

```
cluster1::> volume quota policy rule create -vserver vs0  
-policy-name quota_policy_0 -volume vol0 -type user  
-target user1,DOMXYZ\user2,23457,S-126-098-567,/vol/vol0/qtree1/file2.txt  
-qtree qtree1
```

## See Also

vserver name-mapping   volume quota modify

---

## volume quota policy rule delete

Delete an existing quota rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume quota policy rule delete` command deletes a quota policy rule. This command is not supported on Infinite Volumes. You must enter the following information to delete a quota policy rule:

- Vserver name
- Quota policy name
- Volume name
- Quota target type
- Target to which the rule applies
- Qtree to which the rule applies

Note:

If the rule being deleted belongs to the quota policy that is currently assigned to the Vserver, enforcement of the rule on the volume must be terminated by performing a quota off and on or a quota resize operation using the "`volume quota modify`" command.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver containing the quota policy for which you are deleting a rule.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy in which you are deleting a rule.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume for which you are deleting a rule.

---

**-type** {tree|user|group} - Type

This parameter specifies the quota target type for the rule.

**-target** <text> - Target

This parameter specifies the target to which the quota policy rule applies.

**-qtree** <qtree name> - Qtree Name

This parameter specifies the name of the qtree for which you are deleting a rule.

## Examples

The following example deletes a quota policy rule on Vserver vs1 for the quota policy named quota\_policy\_1. This quota policy applies to the group named engr for the qtree named qtree1 on volume vol1.

```
cluster1::> volume quota policy rule delete -vserver vs1  
-policy-name quota_policy_1 -volume vol1 -type group -target engr  
-qtree qtree1
```

## See Also

volume quota modify

---

## volume quota policy rule modify

Modify an existing quota rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command can be used to modify the following attributes of a quota policy rule:

- User mapping
- Hard disk limit
- Hard file limit
- Threshold for disk limit
- Soft disk limit
- Soft file limit

Note:

If the rule being modified belongs to the quota policy that is currently assigned to the Vserver, rule enforcement on the volume must be enabled by performing a quota off and on or a quota resize operation using the "volume quota modify" command.

This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver containing the quota policy for which you are modifying a rule.

**-policy-name** <text> - Policy Name

This parameter specifies the name of the quota policy in which you are modifying a rule.

**-volume** <volume name> - Volume Name

This parameter specifies the name of the volume for which you are modifying a rule.

**-type** {tree|user|group} - Type

---

This parameter specifies the quota target type for the rule you are modifying.

**-target** <text> - Target

This parameter specifies the target to which the quota policy rule applies. If the target is a user, the user ID or username must be the same one that was used to create the quota. The same restriction is there for both group ID or groupname and Windows SID or Windows account name.

**-qtree** <qtree name> - Qtree Name

This parameter specifies the name of the qtree to which the quota policy rule applies.

**[-user-mapping** {on|off}] - User Mapping

This parameter optionally modifies the user mapping for a user quota rule. The value for this parameter can be modified only for quota policy rules of type user. A value of "on" can be specified for this parameter only if the quota target is a unix user name or a Windows user name and cannot be specified for multi-user quota targets. If this parameter is "on", the unix user name specified as the quota target will be mapped to the corresponding Windows user name or vice-versa and quota accounting will be performed for the users together.

**[-disk-limit** {<size>|-}] - Disk Limit

This parameter optionally modifies the hard limit for the disk space that can be consumed by the quota target. The default unit for the disk limit is assumed to be Kilobytes if no units are specified. The value that you specify for this parameter should be greater than or equal to the threshold and soft disk limit. A disk limit of unlimited can be specified with a "-" for this parameter.

**[-file-limit** {<integer>|-}] - Files Limit

This parameter optionally modifies the hard limit for the number of files permitted on the quota target. The value that you specify for this parameter should be greater than or equal to the soft file limit. A file limit of unlimited can be specified with a "-" for this parameter.

**[-threshold** {<size>|-}] - Threshold for Disk Limit

This parameter optionally modifies the disk limit threshold for the quota target. The default unit for the disk limit threshold is assumed to be Kilobytes if no units are specified. The value that you specify for this parameter should be greater than or equal to the soft disk limit and equal to or less than the disk limit. A threshold limit of unlimited can be specified with a "-" for this parameter.

**[-soft-disk-limit** {<size>|-}] - Soft Disk Limit

This parameter optionally modifies the soft limit for the disk space that can be consumed by the quota target. The default unit for the soft disk limit is assumed to be Kilobytes if

---

no units are specified. The value that you specify for this parameter should be equal to or less than the threshold and the disk limit. A soft disk limit of unlimited can be specified with a "-" for this parameter.

**[-soft-file-limit {<integer>|-}]** - Soft Files Limit

This parameter optionally modifies the soft limit for the number of files permitted on the quota target. The value that you specify for this parameter should be equal to or less than the file limit. A soft file limit of unlimited can be specified with a "-" for this parameter.

## Examples

The following example modifies a quota policy rule for the quota policy named `quota_policy_0`. This quota policy exists on Vserver `vs0` and applies to the user named `myuser` for qtree named `qtree1` on volume `vol0`. The user mapping is turned on, the hard disk limit is set to 20 GB and the hard file limit is set to 100,000 files.

```
cluster1::> volume quota policy rule modify -vserver vs0
-policy-name quota_policy_0 -volume vol0 -type user -target myuser
-qtree qtree1 -user-mapping on -disk-limit 20GB -file-limit 100000
```

## See Also

`volume quota modify`

---

## volume quota policy rule show

Display the quota rules

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the following information about quota policy rules by default.

- Vserver name
- Quota policy name
- Volume name
- Type of quota policy rule
- Target of the quota policy rule
- Qtree name
- User mapping
- Hard disk limit
- Soft disk limit
- Hard file limit
- Soft file limit
- Threshold for disk limit

This command is not supported on Infinite Volumes.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

---

**[-vserver <vserver name>]** - Vserver

If this parameter is specified, the command displays information about quota rules for the quotas contained on volumes on the specified Vserver.

**[-policy-name <text>]** - Policy Name

If this parameter is specified, the command displays information about quota rules for the specified quota policy.

**[-volume <volume name>]** - Volume Name

If this parameter is specified, the command displays information about quota rules for the quota policy associated with the specified volume.

**[-type {tree|user|group}]** - Type

If this parameter is specified, the command displays information about quota rules for the specified quota type.

**[-target <text>]** - Target

If this parameter is specified, the command displays information about quota rules for the specified target.

**[-qtree <qtree name>]** - Qtree Name

If this parameter is specified, the command displays information about quota rules for the specified qtree.

**[-user-mapping {on|off}]** - User Mapping

If this parameter is specified, the command displays information about quota rules having the specified user-mapping value.

**[-disk-limit {<size>|-}]** - Disk Limit

If this parameter is specified, the command displays information about quota rules having the specified hard disk limit.

**[-file-limit {<integer>|-}]** - Files Limit

If this parameter is specified, the command displays information about quota rules having the specified hard file limit.

**[-threshold {<size>|-}]** - Threshold for Disk Limit

If this parameter is specified, the command displays information about quota rules having the specified disk limit threshold.

**[-soft-disk-limit {<size>|-}]** - Soft Disk Limit



---

If this parameter is specified, the command displays information about quota rules having the specified soft disk limit.

**[-soft-file-limit {<integer>|-}] - Soft Files Limit**

If this parameter is specified, the command displays information about quota rules having the specified soft file limit.

**Examples**

The following example displays information about all the quota policy rules in a cluster. There is one user rule that exists on Vserver vs0 for the quota policy named quota\_policy\_0. This quota policy applies to the user named myuser for qtree named qtree0 on volume vol0.

```
cluster1::> volume quota policy rule show
Vserver: vs0      Policy: quota_policy_0      Volume: vol0
```

Type	Target	Qtree	User Mapping	Disk Limit	Disk Limit	Soft Files Limit	Soft Files Limit	Threshold
-----	-----	-----	-----	-----	-----	-----	-----	-----
tree	myuser	qtree0	on	20GB	18GB	100000	80000	16GB

---

## volume snapshot compute-reclaimable

Calculate the reclaimable space if specified snapshots are deleted

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `volume snapshot compute-reclaimable` command calculates the volume space that can be reclaimed if one or more specified Snapshot copies are deleted.

This command is available only at the advanced or higher privilege level. The command heavily uses system's computational resources so it can reduce the performance for client requests and other system processes. Therefore, the queries that use query operators (\*, |, etc.), are disabled for this command. You should not specify more than three Snapshot copies per query. Snapshot copies must be specified as a comma-separated list with no spaces after the commas.

This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume

This specifies the volume for which reclaimable space is to be calculated.

**-snapshots** <snapshot name>, ... - Snapshots

This specifies one or more than one Snapshot copies that are to be considered for deletion. If you list more than one Snapshot copy, specify a comma-separated list with no spaces after the commas.

### Examples

The following example calculates the space that can be reclaimed if the Snapshot copy named `hourly.2008-01-10_1505` is deleted on a volume named `vol3`, which is a part of the Vserver named `vs0`:

```
cluster1::*> volume snapshot compute-reclaimable -vserver vs0  
-volume vol3 -snapshots hourly.2008-01-10_1505
```

---

## volume snapshot create

Create a snapshot

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot create` command creates a Snapshot copy of a specified volume.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver that contains the volume on which the snapshot is to be created.

**-volume** <volume name> - Volume

This specifies the volume where a Snapshot copy is to be created.

**-snapshot** <snapshot name> - Snapshot

This specifies the name of the Snapshot copy that is to be created.

**[-comment** <text>] - Comment

This optionally specifies a comment for the Snapshot copy.

**[-foreground** {true|false}] - Foreground Process

If you use this option and select false, the Snapshot copy creation process runs in the background. If you use this option and select true, the Snapshot copy creation process runs in the foreground. This option applies only to Infinite Volumes, and is ignored for other volumes. The default is true.

**[-snapmirror-label** <text>] - Label for SnapMirror Operations

If you specify this option, the Snapshot copy is created with the SnapMirror Label that you specify. If this option is not specified, the Snapshot copy is created with no SnapMirror Label. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

### Examples

---

The following example creates a Snapshot copy named `vol3_snap` on a volume named `vol3` on a Vserver named `vs0`. The Snapshot copy is given the comment "Single snapshot" and the operation runs in the background.

```
cluster1::> volume snapshot create -vserver vs0 -volume vol3 -snapshot  
vol3_snapshot -comment "Single snapshot" -foreground false
```

## volume snapshot delete

Delete a snapshot

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot delete` command deletes a Snapshot copy from a specified volume.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver that contains the volume on which the specified Snapshot copy is saved.

**-volume** <volume name> - Volume

This specifies the volume from which a Snapshot copy is to be deleted.

**-snapshot** <snapshot name> - Snapshot

This specifies the Snapshot copy that is to be deleted.

**[-foreground {true|false}]** - Foreground Process

If you use this option and set it to `false`, the delete operation runs as a background process. If you specify this option and set it to `true`, the operation runs as a foreground process. This option applies only to Infinite Volumes, and is ignored for other volumes. The default is `true`.

**[-force {true}]** - Force Delete (privilege: advanced)

If you use this switch, the Snapshot copy is immediately deleted without generating any confirmation messages. If you do not use this option the operation generates confirmation messages. Passing in a value of `true` is supported, but not required. The `force` switch is typically used for scripting applications where users cannot directly confirm the delete operation.

---

**[-ignore-owners [true]]** - Ignore Snapshot Owners (privilege: advanced)

If you use this switch, the command ignores other processes that might be accessing the Snapshot copy. If you do not use this option the operation exhibits default behavior and checks the owners tags before allowing the deletion to occur. Passing in a value of true is supported, but not required.

## Examples

The following example deletes a Snapshot copy named vol3\_daily from a volume named vol3 on a Vserver named vs0:

```
cluster1::> volume snapshot delete -vserver vs0 -volume vol3 -snapshot vol3_daily
```

## volume snapshot modify

Modify snapshot attributes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume snapshot modify` command enables you to change the text comment associated with a Snapshot copy.

This command is not supported on Infinite Volumes.

## Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver that contains the volume on which the specified Snapshot copy is saved.

**-volume** <volume name> - Volume

This specifies the volume whose Snapshot copy is to be modified.

**-snapshot** <snapshot name> - Snapshot

This specifies the Snapshot copy whose text comment is to be modified.

**[-comment <text>]** - Comment

This specifies the new comment for the Snapshot copy.

**[-snapmirror-label <text>]** - Label for SnapMirror Operations

---

This specifies the SnapMirror Label for the Snapshot copy. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination. If an empty label ("" ) is specified, the existing label will be deleted.

## Examples

The following example modifies the comment of a Snapshot copy named vol3\_snapshot of a volume named vol3 on a Vserver named vs0. The comment is changed to "Pre-upgrade snapshot".

```
cluster1::> volume snapshot modify -vserver vs0 -volume vol3
-snapshot vol3_snapshot -comment "Pre-upgrade snapshot"
```

## volume snapshot partial-restore-file

Restore part of a file from a snapshot

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume snapshot partial-restore-file` command enables you to restore a range of bytes in a file from the version of the file saved in the Snapshot copy. This command is intended to be used to restore particular pieces of LUNs and NFS or CIFS container files that are used by a host to store multiple sources of data. For example, a host may be storing multiple user databases in the same LUN. A partial file restore can be used to restore one of those databases in the LUN without touching other databases stored in the LUN. This command is not intended for restoring parts of normal user-level files that are stored in the volume. You should use `volume snapshot restore-file` command to restore normal user-level files. The volume for the partial-restore should be online during this operation.

This command is not supported on Infinite Volumes.

## Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver which contains the volume.

**[-volume** <volume name>] - Volume Name

This specifies the volume in which the Snapshot copy is saved.

**-snapshot | -s** <snapshot name> - Snapshot Name

---

This specifies the Snapshot copy which contains the version of file from which a range of bytes is restored. The source file must be present in the Snapshot copy.

**-path <text>** - Filepath

This specifies the path to the file which is partially restored from the Snapshot copy. The `-path` option can be an absolute path or a relative path. If the `-path` option starts with `/vol/`, it is an absolute path. `/vol/` should be followed by the full path to the file inside the volume. If the `-volume` option is specified and you specify an absolute path, then the volume name in the path should match the value of `-volume` option. Paths which do not start with `/vol/` are relative paths to the file. For relative paths, you should specify the `-volume` option so that the file is searched and restored from the Snapshot copy of the specified volume. If you specify a relative path and do not specify the `-volume` then the file is searched and restored from the Snapshot copy of the root volume. The destination file must be present in the active file system.

For example, if you need to partially restore a file `foo.txt` from volume `vol3` then the absolute path to this file is `/vol/vol3/foo.txt`. If you want to specify a relative path to `foo.txt`, then you should set `-volume` to `vol3` and set `-path` to `foo.txt`.

**-start-byte <integer>** - Starting Byte Offset (Multiple of 4096)

This specifies the starting byte offset in the file to partially restore. The first byte of the file is byte zero. The start byte must be a multiple of 4096. In addition, the start byte must not exceed the size of the source or destination file.

**-byte-count <integer>** - Number of Bytes to Restore (Multiple of 4096)

This specifies the total number of bytes to restore, beginning at the `-start-byte` value. The `-byte-count` option must be a multiple of 4096. The maximum number of bytes that can be restored is 16 MB. The byte count must not exceed the range of the source or destination file.

## Examples

The following example restores first 4096 bytes in the file `foo.txt` inside the volume `vol3` from the Snapshot copy `vol3_snap`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume vol3
-snapshot vol3_snap -path /vol/vol3/foo.txt -start-byte 0 -byte-count 4096
```

## See Also

`volume snapshot restore-file`

---

## volume snapshot rename

Rename a snapshot

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot rename` command renames a Snapshot copy.

Note:

You cannot rename a Snapshot copy that is created as a reference copy during the execution of the `volume copy` or `volume move` commands.

This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver that contains the volume on which the specified Snapshot copy is to be renamed

**-volume** <volume name> - Volume

This specifies the volume that contains the Snapshot copy to be renamed.

**-snapshot** <snapshot name> - Snapshot

This specifies the Snapshot copy that is to be renamed.

**-new-name** <snapshot name> - Snapshot New Name

This specifies the new name for the Snapshot copy.

### Examples

The following example renames a Snapshot copy named `vol3_snap` on a volume named `vol3` and a Vserver named `vs0`. The Snapshot copy is renamed to `vol3_snap_archive`.

```
cluster1::> volume snapshot rename -vserver vs0 -volume vol3  
-snapshot vol3_snap -new-name vol3_snap_archive
```

### See Also



---

volume copy   volume move

---

## volume snapshot restore-file

Restore a file from a snapshot

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot restore-file` command enables you to restore a single file to a version saved in the Snapshot copy. You can restore a file over an existing copy of the file in the parent read-write volume or to a different location within the same parent read-write volume. If the destination file for the restore operation does not exist, a new file is created with the same version as the one saved in the Snapshot copy. If the destination file for the restore operation exists, then it is overwritten by the version from the Snapshot copy. This operation is used to restore normal user-level files and LUNs. The command fails if you try to restore directories (and their contents) and files with NT streams. During the restore operation the parent read-write volume should remain online. The command fails if the destination path for the restore operation is in a different volume than the source volume.

This command is not supported on Infinite Volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver which contains the volume.

**[-volume** <volume name>] - Volume Name

This specifies the volume which contains the specified Snapshot copy.

**-snapshot | -s** <snapshot name> - Snapshot Name

This specifies the Snapshot copy from which the file is restored.

**-path** <text> - Filepath

This specifies the path to the file which is restored from the Snapshot copy. The `-path` option can specify an absolute path or a relative path to the file. If the `-path` option starts with `/vol/`, it is an absolute path. `/vol/` should be followed by the full path to file inside the volume. If `-volume` option is specified and you specify an absolute path, then the volume name in the path should match the value of option `-volume`. Paths which do not start with `/vol/` are relative paths to the file. For relative paths, you should specify the `-volume` option so that the file is searched and restored from the Snapshot copy

---

of the specified volume. If you specify a relative path and do not specify the `-volume` option then the file is searched and restored from the Snapshot copy of the root volume.

For example, if you need to restore a file `foo.txt` from volume `vol3` then the absolute path to this file is `/vol/vol3/foo.txt`. If you want to specify a relative path to the file `foo.txt`, then you should set `-volume` to `vol3` and set `-path` to `foo.txt`.

#### **`[-restore-path | -r <text>]` - Restore Filepath**

This option specifies the destination location inside the volume where the file is restored. If you do not specify this option, the file is restored at the same location referred by `-path` option. If you specify `-restore-path` option, then it should refer to a location within the same volume which contains the source file. The `-restore-path` option can be an absolute or relative path. If you specify an absolute path and specify `-volume` option then the volume in the path should match the specified volume. If you specify a relative path, then you should specify `-volume` option. If you do not specify `-volume`, the file is restored in the root volume.

#### **`[-split-disabled [true]]` - Disable Space Efficient LUN Splitting**

If you use this option and set it to `true`, space efficient LUN clone split is not allowed during the restore operation. If you use this option and set it to `false` or do not use this option, then space efficient LUN clone split is allowed during the restore operation.

## **Examples**

The following example restores a file `foo.txt` from the Snapshot copy `vol3_snap` inside the volume `vol3` contained in a Vserver `vs0`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol3 -snapshot
vol3_snap -path /vol/vol3/foo.txt
```

## **volume snapshot restore**

Restore the volume to a snapshot.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## **Description**

The `volume snapshot restore` command restores a Snapshot copy to be the read-write parent volume for the volume family. This replaces the current working copy of the volume with the Snapshot copy that results in a loss of all changes made since the Snapshot copy was created.

Note:

---

You should manually update all the SnapMirror relationships of a volume immediately after you restore its Snapshot copy. Not doing so can result in unusable SnapMirror relationships that must be deleted and re-created.

Before running this command on an Infinite Volume, unmount the volume. Any namespace mirror constituents present in the system are resynchronized to the restored Snapshot copy.

After the restore is complete, the size of the flexible volume will be set to either the current volume size or the snapshot size - whichever is greater.

## Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver that contains the volume on which the specified Snapshot copy to be restored is saved.

**-volume** <volume name> - Volume

This specifies the parent read-write volume whose Snapshot copy is to be restored to take its place.

**-snapshot** <snapshot name> - Snapshot

This specifies the Snapshot copy that is to be restored to be the read-write parent volume.

**[-force [true]]** - Force Restore

If you use this option, the Snapshot copy is immediately restored without generating any confirmation messages. If you do not use this option the operation generates confirmation messages. Passing in a value of true is supported, but not required. The `force` option is typically used for scripting applications where there is no user to confirm the operation.

**[-preserve-lun-ids {true|false}]** - Preserve LUN Identifiers

This option enables you to select whether the Snapshot copy restore needs to be non-disruptive to clients due to LUN identifiers changing. If you use this option and set it to true, or choose to not use this option at all, the `volume snapshot restore` command fails if the system determines that it cannot be non-disruptive with regards to LUN identifiers. If you use this option and set it to false the restore operation proceeds even if this might cause client-visible effects. In this case, administrators should take the LUNs offline before proceeding.

## Examples

---

The following example restores a Snapshot copy named `vol3_snap_archive` to be the parent read-write volume for the volume family. The existing read-write volume is named `vol3` and is located on a Vserver named `vs0`:

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3  
-snapshot vol3_snap_archive
```

## volume snapshot show

Display a list of snapshots

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot show` command displays information about Snapshot copies. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays a table with the following information about all the available Snapshot copies:

- Vserver name
- Volume name
- Snapshot copy name
- State
- Size
- Percentage of total blocks in the parent volume
- Percentage of used blocks in the parent volume

To display a detailed list view with additional information, run the command and select the `-instance` view. In addition to the above mentioned information about the Snapshot copies, the detailed list view provides the following additional information:

- Creation time
- Snapshot busy
- List of the Snapshot copy's owners
- Comment associated with the Snapshot copy
- SnapMirror Label associated with the Snapshot copy
- 7-Mode Snapshot

- 
- Constituent Snapshot

At the advanced or higher privilege level the detailed view provides the following additional information:

- Snapshot copy's Dataset ID
- Snapshot copy's master Dataset ID
- Number of consistency points in the Snapshot copy
- Internal status of the Snapshot copy
- File system version
- File system block format
- Physical Snap ID
- Logical Snap ID
- Database record owner
- Snapshot tags
- Instance UUID
- Version UUID
- Node

The list view is automatically enabled if a single Snapshot copy is specified by using the `-vserver`, `-volume` and `-snapshot` options together.

A preformatted query for displaying the time-related information is available by specifying the `-time` format specifier. This displays a table that contains the following fields for all the available Snapshot copies:

- Vserver name
- Volume name
- Snapshot copy name
- Creation time

By using the `-fields` option you can choose to print only the certain fields in the output. This presents the selected fields in a table view. This is ideal when you want additional information to be different from the information that is provided by the default table view, but would like it in a format which is visually easy to compare.

---

You can specify additional parameters to display the information that matches only those parameters. For example, to display information only about Snapshot copies of the load-sharing volumes, run the command with the `-volume-type LS` parameter. If you specify multiple filtering parameters, only those Snapshot copies that match all the specified parameters are displayed.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-time ]**

If the `-time` format is specified, the command displays time related information about all entries.

| **[-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you use this parameter, the Snapshot copies located only on the specified Vserver will be displayed.

**[-volume <volume name>]** - Volume

If you use this parameter only Snapshot copies located on the specified volume will be displayed.

**[-snapshot <snapshot name>]** - Snapshot

If you use this parameter only Snapshot copies matching the specified name will be displayed.

**[-dsid <integer>]** - Snapshot Data Set ID (privilege: advanced)

If this parameter is specified, the command displays information only about the Snapshot copy that has the specified data set ID.

**[-msid <integer>]** - Snapshot Master Data Set ID (privilege: advanced)

If this parameter is specified, the command displays information only about the Snapshot copy that has the specified master data set ID.

**[-create-time <Date>]** - Creation Time

---

If this parameter is specified, the command displays information only about the Snapshot copies that match the specified creation time.

**[-busy {true|false}]** - Snapshot Busy

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified busy status.

**[-owners <text>, ...]** - List of Owners

If this parameter is specified, the command displays information only about the Snapshot copies that are owned by the specified list of owners.

**[-size {<integer>[KB|MB|GB|TB|PB]}]** - Snapshot Size

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified size. The size is specified as a character specifying the unit of measurement followed by a number specifying the size in the mentioned unit of measurement: k (kilobytes), m (megabytes), g (gigabytes), or t (terabytes). If the unit of measurement is not specified, bytes are used as the unit, and the specified number is rounded up to the nearest 4 KB. You may also use an inequality such as >10mb as input.

**[-blocks <percent>]** - Percentage of Total Blocks

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified percentage of total blocks on their parent volumes. You may also use an inequality such as >10 as input.

**[-usedblocks <percent>]** - Percentage of Used Blocks

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified percentage of used blocks on their parent volumes. You may also use an inequality such as >10 as input.

**[-cpcount <integer>]** - Consistency Point Count (privilege: advanced)

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified number of consistency points. You may also use an inequality such as <100 as input.

**[-internal-status <text>]** - Internal Status (privilege: advanced)

If this parameter is specified, the command displays information only about the Snapshot copies that have the specified internal status. You may also specify an equality such as != as input.

**[-comment <text>]** - Comment



If this parameter is specified, the command displays information only about the Snapshot copies that have the specified comment text. You may also specify an inequality such as "!" as input.

**[-fs-version <text>]** - File System Version (privilege: advanced)

If you use this parameter the only Snapshot copies displayed are those that were created when the file system was of a specific release. This parameter is helpful especially when you need to upgrade to newer software release and want to know the Snapshot copies that will be impacted by the upgrade process.

**[-is-7-mode {true|false}]** - 7-Mode Snapshot

If you use this parameter only those Snapshot copies which have the specified value are shown. This value is true for the Snapshot copies that exist on the volume that was in 7-mode configuration and then transitioned to 10-mode configuration. In such a scenario, the volume is in 10-mode configuration and the existing Snapshot copies are still in the 7-mode configuration.

**[-snapmirror-label <text>]** - Label for SnapMirror Operations

If you use this parameter, only those Snapshot copies that have the specified SnapMirror Label value are shown.

**[-state {valid|invalid|partial}]** - Snapshot State

If you use this parameter only those Snapshot copies which have the specified state will be shown.

**[-is-constituent {true|false}]** - Constituent Snapshot

If you use this parameter, only those Snapshot copies whose parent volume is a constituent volume of an Infinite Volume will be shown.

**[-node <nodename>]** - Node (privilege: advanced)

If you use this parameter only those Snapshot copies that are located on the specified storage system are shown.

## Examples

The following example displays detailed information about all Snapshot copies of a volume named vol1:

```
cluster1::> volume snapshot show -volume vol1
```

Vserver	Volume	Snapshot	State	Size	---Blocks---	Total%	Used%
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	mirror_ref_snapshot_2153852611	valid	184KB		20%	0%
		daily.2008-10-18_0010	valid	236KB		24%	0%
		daily.2008-10-19_0010	valid	188KB		20%	0%
		hourly.2008-10-19_0505	valid	184KB		20%	0%
		hourly.2008-10-19_0605	valid	184KB		20%	0%
		hourly.2008-10-19_0705	valid	184KB		20%	0%

---

	hourly.2008-10-19_0805	valid	184KB	20%	0%
	weekly.2008-10-07_0015	valid	220KB	23%	0%
	weekly.2008-10-14_0015	valid	232KB	23%	0%
vs1	voll_dr				
	__mirror_ref_snapshot_2153849126	valid	72KB	9%	0%
	__mirror_ref_snapshot_2153852611	valid	0B	0%	0%
	daily.2008-10-18_0010	valid	236KB	24%	0%
	daily.2008-10-19_0010	valid	188KB	20%	0%
	hourly.2008-10-19_0305	valid	188KB	20%	0%
	hourly.2008-10-19_0405	valid	188KB	20%	0%
	hourly.2008-10-19_0505	valid	184KB	20%	0%
	hourly.2008-10-19_0605	valid	184KB	20%	0%
	weekly.2008-10-07_0015	valid	220KB	23%	0%
	weekly.2008-10-14_0015	valid	232KB	24%	0%

16 entries were displayed.

---

## volume snapshot autodelete modify

Modify autodelete settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot autodelete modify` command enables you to modify Snapshot autodelete and LUN clone autodelete policy settings. Based on the defined policy, automatic deletion of Snapshot copies and LUN clones is triggered. Automatic deletion of Snapshot copies and LUN clones is useful when you want to automatically reclaim space consumed by the Snapshot copies and LUN clones from the volume when it is low in available space. LUN clone autodelete follows Snapshot copy autodelete. This command works only on a read-write parent volume. You cannot setup automatic Snapshot copy deletion and automatic LUN clone deletion for Infinite Volumes and read-only volumes.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the volume is located.

**-volume** <volume name> - Volume Name

This specifies the volume whose autodelete policy has to be modified.

**[-enabled {true|false}]** - Enabled

This option specifies whether automatic deletion of Snapshot copies and LUN clones is enabled or disabled. If set to true, automatic deletion of Snapshot copies and LUN clones is enabled. If set to false, automatic deletion of Snapshot copies and LUN clones is disabled.

**[-commitment {try|disrupt|destroy}]** - Commitment

This option specifies which Snapshot copies and LUN clones can be automatically deleted to reclaim back space.

When set to try, the Snapshot copies which are not locked by any application and the LUN clones which are not configured as preserved are deleted.

When set to disrupt, the Snapshot copies which are not locked by data backing functionalities (such as volume clones, LUN clones and file clones) and LUN clones which are not configured as preserved are deleted. In the disrupt mode, the Snapshot

---

copies locked by data protection utilities such as Snapmirror and Volume Move can be deleted. If such a locked Snapshot copy is deleted during the data transfer, the transfer is aborted.

When set to destroy, the Snapshot copies locked by the data backing functionalities are deleted. In addition, all the LUN clones in the volume are deleted.

**[-defer-delete {scheduled|user\_created|prefix|none}]** - Defer Delete

This option determines the order in which Snapshot copies can be deleted.

Possible values are as follows:

- When set to scheduled, scheduled Snapshot copies are the last to be deleted.
- When set to user\_created, user Snapshot copies are the last to be deleted.
- When set to prefix, Snapshot copies matching a certain prefix are the last to be deleted.
- When set to none, no defer deletion order is honored.

This option is not applicable for LUN clones.

**[-delete-order {newest\_first|oldest\_first}]** - Delete Order

This option specifies if the oldest Snapshot copy and the oldest LUN clone or the newest Snapshot copy and the newest LUN clone are deleted first.

**[-defer-delete-prefix <text>]** - Defer Delete Prefix

This option specifies the prefix string for the `-defer-delete prefix` parameter. The option is not applicable for LUN clones.

**[-target-free-space <percent>]** - Target Free Space

This option specifies the free space percentage at which the automatic deletion of Snapshot copies and LUN clones must stop. Depending on the `-trigger` Snapshot copies and LUN clones are deleted until you reach the target free space percentage.

**[-trigger {volume|snap\_reserve|space\_reserve}]** - Trigger

This option specifies the condition which starts the automatic deletion of Snapshot copies and LUN clones.

Setting this option to volume triggers automatic deletion of Snapshot copies and LUN clones when the volume reaches threshold capacity and the volume space reserved for Snapshot copies is exceeded.

Setting the option to snap\_reserve triggers automatic deletion of Snapshot copies when the space reserved for Snapshot copies reaches threshold capacity.

---

Setting the option to `space_reserve` triggers automatic deletion of Snapshot copies when reserved space in the volume reaches threshold capacity and the volume space reserved for Snapshot copies is exceeded.

The threshold capacity is determined by the size of the volume as follows:

- If the volume size is less than 20 GB, the autodelete threshold is 85%.
- If the volume size is equal to or greater than 20 GB and less than 100 GB, the autodelete threshold is 90%.
- If the volume size is equal to or greater than 100 GB and less than 500 GB, the autodelete threshold is 92%.
- If the volume size is equal to or greater than 500 GB and less than 1 TB, the autodelete threshold is 95%.
- If the volume size is equal to or greater than 1 TB, the autodelete threshold is 98%.

#### **`[-destroy-list <text>]` - Destroy List**

This option specifies a comma separated list of data backing functions which are affected if the automatic deletion of the Snapshot copy backing that service is triggered. The possible values for this option are `lun_clone`, `fileclone`, `lun_clone,sfsr`, `vol_clone`, `cifs_share`, or `none`. Except `none`, all the other options can be combined as a comma separated list. Note that `"lun_clone"`, `"file_clone"` and `"sfsr"` individually are not valid values. Only pairs `"lun_clone,file_clone"` and `"lun_clone,sfsr"` are supported.

If you specify `vol_clone`, the cloned volume backed by the Snapshot copy is deleted.

If you specify `lun_clone`, and the LUN is in the process of being cloned when autodelete is triggered, the cloning operation is aborted. Any access to this LUN will result in an error being reported to the client.

If you specify `file_clone`, and the file cloning operation is in progress when autodelete is triggered, the cloning operation is aborted. Any access to this file will result in an error being reported to the client.

If you specify `sfsr`, and the file restore is in progress when autodelete is triggered, the restore operation is aborted.

If the Snapshot copy is locked either by a `lun_clone` or `file_clone` or both, the `-destroy-list` must be set to `lun_clone,file_clone`.

If the Snapshot copy is locked either by a `lun_clone` or `sfsr` operation or both, the `-destroy-list` must be set to `lun_clone,file_clone`. The options `file_clone` and `sfsr` are equivalent to each other.

If you set `-destroy-list` to `lun_clone,file_clone` and the Snapshot copy is backing a file clone or `sfsr` operation, both the operations are aborted. This is also the case when you set `-destroy-list` to `lun_clone,sfsr`.

---

LUN clone autodelete is applicable only if `-destroy-list` contains `lun_clone`.

## Examples

The following example enables Snapshot autodelete and sets the trigger to `snap_reserve` for volume `vol3` which is part of the Vserver `vs0`:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol3 -enabled  
true -trigger snap_reserve
```

The following example enables Snapshot autodelete and LUN clone autodelete for volume `vol3` which is part of the Vserve `vs0`:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol3 -enabled  
true -trigger volume -commitment try -delete-order oldest_first -destroy-list  
lun_clone,file_clone
```

---

## volume snapshot autodelete show

Display autodelete settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot autodelete show` command displays information about Snapshot autodelete policies. The command output depends on the parameters specified with the command. If no parameters are specified, the command displays a table with the following information about all the available Snapshot autodelete policies:

- Vserver name
- Volume name
- Option name
- Option value

To display a detailed list view with additional information, run the command and select the `-instance` view. The detailed list view provides the following information:

- Vserver name
- Volume name
- Enabled
- Commitment
- Defer Delete
- Delete Order
- Defer Delete Prefix
- Target Free Space
- Trigger
- Destroy List
- Is Constituent Volume

By using the `-fields` option you can choose to print only the certain fields in the output. This presents the selected fields in a table view. This is ideal when you want

---

additional information to be different from the information that is provided by the default table view, but would like it in a format which is visually easy to compare.

You can specify additional parameters to display the information that matches only those parameters. For example, to display information only about Snapshot autodelete policies which are enabled, run the command with `-enabled true` parameter. If you specify multiple filtering parameters, only those policies that match all the specified parameters are displayed.

## Parameters

**{ [-fields <fieldname>, ...]**

This option allows you to print only certain fields in the output.

**| [-instance ] }**

This option allows you to print a detailed list view.

**[-vserver <vserver name>]** - Vserver Name

If this parameter and the `-volume` parameter are specified, the command displays detailed autodelete policy information about the specified volume. If this parameter is specified by itself, the command displays autodelete policy information about volumes on the specified Vserver.

**[-volume <volume name>]** - Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed autodelete policy information about the specified volume. If this parameter is specified by itself, the command displays autodelete policy information about all volumes matching the specified name.

**[-enabled {true|false}]** - Enabled

If this parameter is specified, the command displays information about autodelete policies that match the specified parameter value.

**[-commitment {try|disrupt|destroy}]** - Commitment

If this parameter is specified, the command displays information about autodelete policies that match the specified commitment value.

**[-defer-delete {scheduled|user\_created|prefix|none}]** - Defer Delete

If this parameter is specified, the command displays information about autodelete policies that match the specified defer deletion criterion.

**[-delete-order {newest\_first|oldest\_first}]** - Delete Order



If this parameter is specified, the command displays information about autodelete policies that match the specified deletion order.

**[-defer-delete-prefix <text>]** - Defer Delete Prefix

If this parameter is specified, the command displays information about autodelete policies that match the prefix used for deferring deletion.

**[-target-free-space <percent>]** - Target Free Space

If this parameter is specified, the command displays information about autodelete policies that match the specified target free space.

**[-trigger {volume|snap\_reserve|space\_reserve}]** - Trigger

If this parameter is specified, the command displays information about autodelete policies that match the specified trigger condition.

**[-destroy-list <text>]** - Destroy List

If this parameter is specified, the command displays information about autodelete policies that match the specified value.

**[-is-constituent {true|false}]** - Is Constituent Volume

If this parameter is specified, the command displays information about autodelete policies for the constituent volumes of Infinite Volumes.

### Examples

The following example displays Snapshot autodelete policy settings for volume vol3 which is inside the Vserver vs0:

```
cluster1::> volume snapshot autodelete show -vserver vs0 -volume vol3
```

Vserver	Volume	Option Name	Option Value
vs0	vol3	Enabled	false
		Commitment	try
		Trigger	volume
		Target Free Space	20%
		Delete Order	oldest_first
		Defer Delete	user_created
		Defer Delete Prefix	(not specified)
		Destroy List	none

---

## volume snapshot policy add-schedule

Add a schedule to snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot policy add-schedule` command adds a schedule to a Snapshot policy. You can create a schedule by using the `job schedule cron create` or `job schedule interval create` commands.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which a Snapshot policy schedule is to be added.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy to which a schedule is to be added.

**-schedule** <text> - Schedule Name

This specifies the schedule that is to be added to the Snapshot policy.

**-count** <integer> - Maximum Snapshot Copies for Schedule

This specifies the maximum number of Snapshot copies that can be taken by the specified schedule.

**[-prefix <text>]** - Snapshot Copy Name Prefix for Schedule

This option specifies the prefix with which Snapshot copies will be created for the added schedule. Every schedule has only one prefix. Once a prefix gets associated with a schedule, you cannot update the prefix. If some prefix is already associated with the schedule and you do not specify this parameter, then the previously defined prefix is used. The command fails if you try to update an existing prefix for a schedule. If no prefix is associated with the schedule and you do not specify this parameter, then schedule name is be used as the prefix.

**[-snapmirror-label <text>]** - Label for SnapMirror Operations

This specifies the SnapMirror Label identified with a Snapshot copy when it is created for the added schedule. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

---

## Examples

The following example adds a schedule named midnight to the Snapshot policy named snappolicy\_nightly on Vserver vs0. The schedule can take a maximum of five Snapshot copies.

```
cluster1::> volume snapshot_policy add-schedule -vserver vs0 -policy  
snappolicy_nightly -schedule midnight -count 5
```

## See Also

[job schedule cron create](#) [job schedule interval create](#)

---

## volume snapshot policy create

Create a new snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot policy create` command creates a Snapshot policy. A Snapshot policy includes at least one schedule, up to a maximum of five schedules, and a maximum number of Snapshot copies per schedule. You can create a schedule by using the `job schedule cron create` or `job schedule interval create` commands. When applied to a volume, the Snapshot policy specifies the schedule on which Snapshot copies are taken and the maximum number of Snapshot copies that each schedule can take.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the Snapshot policy is to be created.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy that is to be created.

**-enabled** {true|false} - Snapshot Policy Enabled

This specifies whether the Snapshot policy is enabled.

**[-comment** <text>] - Comment

This option specifies a text comment for the Snapshot policy.

**-schedule1** <text> - Schedule1 Name

This specifies the name of the first schedule associated with the Snapshot policy.

**-count1** <integer> - Maximum Snapshot Copies for Schedule1

This specifies the maximum number of Snapshot copies that can be taken by the first schedule.

**[-prefix1** <text>] - Snapshot Copy Name Prefix for Schedule1

This option specifies the prefix associated with the first schedule. Every schedule has only one prefix. The command fails if you try to update an existing prefix. If you do not

---

specify this parameter and there is no prefix associated with the schedule, the schedule name is used as the prefix. If you do not specify this parameter and there is already a prefix associated with the schedule from a previous invocation of the command, then that prefix is used.

**[-snapmirror-label1 <text>]** - Label for SnapMirror Operations for Schedule1

This specifies the SnapMirror Label of the first schedule associated with the Snapshot policy. Once specified, all Snapshot copies created for that schedule have the SnapMirror Label assigned to them. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

**[-schedule2 <text>]** - Schedule2 Name

This option specifies the name of the second schedule associated with the Snapshot policy. If this parameter is specified, the `-count2` parameter must also be specified.

**[-count2 <integer>]** - Maximum Snapshot Copies for Schedule2

This option specifies the maximum number of Snapshot copies that can be taken by the second schedule. If this parameter is specified, the `-schedule2` parameter must also be specified.

**[-prefix2 <text>]** - Snapshot Copy Name Prefix for Schedule2

This option specifies the prefix associated with the second schedule. If this parameter is specified, `-schedule2` and `-count2` parameters must also be specified. Every schedule has only one prefix. The command fails if you try to update an existing prefix. If you do not specify this parameter and there is no prefix associated with the schedule, the schedule name is used as the prefix. If you do not specify this parameter and there is already a prefix associated with the schedule from a previous invocation of the command, then that prefix is used.

**[-snapmirror-label2 <text>]** - Label for SnapMirror Operations for Schedule2

This specifies the SnapMirror Label of the second schedule associated with the Snapshot policy. Once specified, all Snapshot copies created for that schedule have the SnapMirror Label assigned to them. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

**[-schedule3 <text>]** - Schedule3 Name

This option specifies the name of the third schedule associated with the Snapshot policy. If this parameter is specified, the `-count3` parameter must also be specified.

**[-count3 <integer>]** - Maximum Snapshot Copies for Schedule3

This option specifies the maximum number of Snapshot copies that can be taken by the third schedule. If this parameter is specified, the `-schedule3` parameter must also be specified.

---

**[-prefix3 <text>]** - Snapshot Copy Name Prefix for Schedule3

This option specifies the prefix associated with the third schedule. If this parameter is specified, `-schedule3` and `-count3` parameters must also be specified. Every schedule has only one prefix. The command fails if you try to update an existing prefix. If you do not specify this parameter and there is no prefix associated with the schedule, the schedule name is used as the prefix. If you do not specify this parameter and there is already a prefix associated with the schedule from a previous invocation of the command, then that prefix is used.

**[-snapmirror-label3 <text>]** - Label for SnapMirror Operations for Schedule3

This specifies the SnapMirror Label of the third schedule associated with the Snapshot policy. Once specified, all Snapshot copies created for that schedule have the SnapMirror Label assigned to them. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

**[-schedule4 <text>]** - Schedule4 Name

This option specifies the name of the fourth schedule associated with the Snapshot policy. If this parameter is specified, the `-count4` parameter must also be specified.

**[-count4 <integer>]** - Maximum Snapshot Copies for Schedule4

This option specifies the maximum number of Snapshot copies that can be taken by the fourth schedule. If this parameter is specified, the `-schedule4` parameter must also be specified.

**[-prefix4 <text>]** - Snapshot Copy Name Prefix for Schedule4

This option specifies the prefix associated with the fourth schedule. If this parameter is specified, `-schedule4` and `-count4` parameters must also be specified. Every schedule has only one prefix. The command fails if you try to update an existing prefix. If you do not specify this parameter and there is no prefix associated with the schedule, the schedule name is used as the prefix. If you do not specify this parameter and there is already a prefix associated with the schedule from a previous invocation of the command, then that prefix is used.

**[-snapmirror-label4 <text>]** - Label for SnapMirror Operations for Schedule4

This specifies the SnapMirror Label of the fourth schedule associated with the Snapshot policy. Once specified, all Snapshot copies created for that schedule have the SnapMirror Label assigned to them. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

**[-schedule5 <text>]** - Schedule5 Name

This option specifies the name of the fifth schedule associated with the Snapshot policy. If this parameter is specified, the `-count5` parameter must also be specified.

---

**[-count5 <integer>]** - Maximum Snapshot Copies for Schedule5

This option specifies the maximum number of Snapshot copies that can be taken by the fifth schedule. If this parameter is specified, the `-schedule5` parameter must also be specified.

**[-prefix5 <text>]** - Snapshot Copy Name Prefix for Schedule5

This option specifies the prefix associated with the fifth schedule. If this parameter is specified, `-schedule5` and `-count5` parameters must also be specified. Every schedule has only one prefix. The command fails if you try to update an existing prefix. If you do not specify this parameter and there is no prefix associated with the schedule, the schedule name is used as the prefix. If you do not specify this parameter and there is already a prefix associated with the schedule from a previous invocation of the command, then that prefix is used.

**[-snapmirror-label5 <text>]** - Label for SnapMirror Operations for Schedule5

This specifies the SnapMirror Label of the fifth schedule associated with the Snapshot policy. Once specified, all Snapshot copies created for that schedule have the SnapMirror Label assigned to them. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination.

## Examples

The following example creates a Snapshot policy named `snappolicy_4hrs` on a Vserver named `vs0`. The policy runs on a single schedule named `4hrs` with a prefix `every_4_hour` and has a maximum number of five Snapshot copies.

```
cluster1::> volume snapshot policy create -vserver vs0 -policy snappolicy_4hrs  
-schedule1 4hrs -count1 5 -prefix1 every_4_hour
```

## See Also

`job schedule cron create` `job schedule interval create`

---

## volume snapshot policy delete

Delete a snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot policy delete` command deletes a Snapshot policy.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver on which the Snapshot policy is to be deleted.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy that is to be deleted.

### Examples

The following example deletes a Snapshot policy named `snappolicy_hourly` on Vserver `vs0`:

```
cluster1::> volume snapshot policy delete -vserver vs0 -policy snappolicy_hourly
```

## volume snapshot policy modify-schedule

Modify a schedule within snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `volume snapshot policy modify-schedule` command modifies the maximum number of Snapshot copies that can be taken by a Snapshot policy's schedule.

### Parameters

**-vserver** <vserver name> - Vserver Name



---

This specifies the Vserver on which a Snapshot policy schedule is to be modified.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy whose schedule is to be modified.

**-schedule** <text> - Schedule Name

This specifies the schedule that is to be modified.

**[-newcount <integer>]** - Maximum Snapshot Copies for Schedule

This specifies the maximum number of Snapshot copies that can be taken by the specified schedule.

**[-newsnapmirror-label <text>]** - Label for SnapMirror Operations

This specifies the SnapMirror Label identified with a Snapshot copy when it is created for the specified schedule. The SnapMirror Label is used by the Vaulting subsystem when you back up Snapshot copies to the Vault Destination. If an empty label ("") is specified, the existing label will be deleted.

## Examples

The following example changes the maximum number of Snapshot copies from five to four for a schedule named midnight on a Snapshot policy named snappolicy\_nightly on Vserver vs0:

```
cluster1::> volume snapshot policy modify-schedule -vserver vs0 -policy  
snappolicy_nightly -schedule midnight -newcount 4
```

## volume snapshot policy modify

Modify a snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume snapshot policy modify` command enables you to modify the description associated with a Snapshot policy and whether the policy is enabled or disabled.

## Parameters

**-vserver** <vserver name> - Vserver Name

---

This specifies the Vserver on which the Snapshot policy is to be modified.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy that is to be modified.

**[-enabled {true|false}]** - Snapshot Policy Enabled

This optionally specifies whether the Snapshot policy is enabled.

**[-comment <text>]** - Comment

This specifies the comment text for the Snapshot policy.

**[-snapmirror-labels <text>, ...]** - Label for SnapMirror Operations

This optionally specifies a comma separated list of SnapMirror labels that are applied to the schedules in the Snapshot policy. Each label in the list applies to only one schedule in the Snapshot policy (maximum of 5 SnapMirror labels), the first label applying to the first schedule, the second label applying to the second schedule, and so on. You can have a maximum of five SnapMirror labels, which corresponds to the maximum number of schedules a Snapshot policy can have. If an empty string ("") is specified, the existing labels will be deleted from all the schedules.

## Examples

The following example changes the description of a Snapshot policy named `snappolicy_wknd` on Vserver `vs0` to "Runs only on weekends":

```
cluster1::> volume snapshot policy modify -vserver vs0 -policy snappolicy_wknd -  
comment "Runs only on weekends"
```

## volume snapshot policy remove-schedule

Remove a schedule from snapshot policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume snapshot policy remove-schedule` command removes a schedule from a Snapshot policy.

## Parameters

**-vserver** <vserver name> - Vserver Name

---

This specifies the Vserver on which a Snapshot policy schedule is to be removed.

**-policy** <snapshot policy> - Snapshot Policy Name

This specifies the Snapshot policy from which a schedule is to be removed.

**-schedule** <text> - Schedule Name

This specifies the schedule that is to be removed from the Snapshot policy.

## Examples

The following example removes a schedule named hourly from a Snapshot policy named snappolicy\_daily on Vserver vs0:

```
cluster1::> volume snapshot policy remove-schedule -vserver vs0 -policy  
snappolicy_daily -schedule hourly
```

## volume snapshot policy show

Show snapshot policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `volume snapshot policy show` command displays the following information about Snapshot policies:

- Vserver name
- Snapshot policy name
- Number of schedules in the policy
- Comment for the policy
- Individual schedule names
- Maximum number of Snapshot copies associated with each schedule
- Snapshot copy name prefixes for the schedules
- SnapMirror Labels associated with the schedules

## Parameters

{ [-fields <fieldname>, ...]

---

This option allows you to print only certain fields in the output.

| **[-instance ]** }

This option allows you to print a detailed list view about Snapshot policies.

**[-vserver <vserver name>]** - Vserver Name

If this parameter is specified, the command displays Snapshot policies on the specified Vserver.

**[-policy <snapshot policy>]** - Snapshot Policy Name

If this parameter is specified, the command displays detailed information about the specified Snapshot policy.

**[-enabled {true|false}]** - Snapshot Policy Enabled

If this parameter is specified, the command displays detailed information only about the Snapshot policy or policies that have the specified enabled value.

**[-comment <text>]** - Comment

If this parameter is specified, the command displays information only about the Snapshot policy or policies that have the specified comment.

**[-total-schedules <integer>]** - Total Number of Schedules in this Policy

If this parameter is specified, the command displays information only about the Snapshot policy or policies that have the specified total number of schedules.

**[-schedules <text>, ...]** - Schedule Name

If this parameter is specified, the command displays information only about the Snapshot policy or policies that have the specified list of schedules.

**[-counts <integer>, ...]** - Maximum Snapshots for the Schedule

If this parameter is specified, the command displays information only about the Snapshot policy or policies that have the specified list of maximum numbers of Snapshot copies per schedule.

**[-prefixes <text>, ...]** - Prefix Name

If this parameter is specified, the command displays information only about the Snapshot policy or policies that have the specified list of prefixes.

**[-snapmirror-labels <text>, ...]** - Label for SnapMirror Operations

If this parameter is specified, the command displays information only about the Snapshot policies that have the specified SnapMirror Label. When you specify a list of

---

SnapMirror labels, the command displays all the Snapshot policies that contain any of the SnapMirror Labels specified in the list.

**[-policy-owner <text>]** - Owner of the policy

If this parameter is specified, the command displays information only about the Snapshot policies that have the specified policy owner.

## Examples

The following example displays information about all Snapshot policies:

```
cluster1::> volume snapshot policy show
Vserver: cm
```

Policy Name	Number of Schedules	Is Enabled	Comment
default	3	false	Default policy with hourly, daily & weekly schedules.
Schedule	Count	Prefix	SnapMirror Label
hourly	6	hourly	-
daily	2	daily	-
weekly	2	weekly	-
default-1weekly & 1 weekly schedule.	3	false	Default policy with 6 hourly, 2 daily & 1 weekly schedule.
Schedule	Count	Prefix	SnapMirror Label
hourly	6	hourly	-
daily	2	daily	-
weekly	1	weekly	-
none	0	false	Policy for no automatic snapshots.
Schedule	Count	Prefix	SnapMirror Label
-	-	-	-

```
Vserver: vs0
```

Policy Name	Number of Schedules	Is Enabled	Comment
p1	1	false	-
Schedule	Count	Prefix	SnapMirror Label
weekly	2	weekly	-
p2	2	true	-
Schedule	Count	Prefix	SnapMirror Label
hourly	6	hourly	-
daily	2	daily	-

5 entries were displayed.

---

## vserver context

Set Vserver context

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

Cluster administrators can use the `vserver context` command to login to a specified Vserver with a specified Vserver user name. All subsequent commands will be issued in the context of that Vserver. The role of the cluster administrator will be the same as that of the user name with which the Vserver context was set. The context is valid for the duration of the CLI or Web UI session in which it is specified. The `exit` command can be used to return to the original context.

### Parameters

**-vserver** <vserver> - Vserver

Use this parameter to specify the Vserver.

**[-username** <text>] - Vserver Administrator User Name

Use this parameter to specify a Vserver administrator user name for the context. The default value `vsadmin` is used if one is not specified.

### Examples

The following example sets the CLI context to Vserver `vs0.example.com`. All subsequently issued commands will be executed in the context of that Vserver:

```
cluster1::> vserver context -vserver vs0.example.com
Info: Use 'exit' command to return.
vs0.example.com::>
```

### See Also

`exit`

---

## vserver create

Create a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver create` command creates a Vserver.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the name of the Vserver that is to be created. Use a fully qualified domain name (FQDN) - for example, "data.example.com" - for the Vserver name to reduce name collisions in cluster leagues.

Note:

The name must be 47 characters or less.

**-rootvolume** <volume name> - Root Volume

This specifies the name of the Vserver's root volume, which is created when the Vserver is created. The size of the Vserver's root volume is 1GB

**-aggregate** <aggregate name> - Aggregate

This specifies the storage aggregate that holds the Vserver's root volume.

**-ns-switch** {nis|file|ldap}, ... - Name Service Switch

This specifies the sources that are searched for name service information and the order in which they are searched. Possible values include nis, file, and ldap. This parameter provides the functionality of the `/etc/nsswitch.conf` file on UNIX systems; see the UNIX man page for `nsswitch.conf(5)` for more information.

**[-nm-switch** {file|ldap}, ...] - Name Mapping Switch

This specifies the sources that are searched for name mapping information and the order in which they are searched. Possible values include file and ldap. The default value is file.

**-rootvolume-security-style** {unix|ntfs|mixed|unified} - Root Volume Security Style

---

This specifies the security style for the Vserver's root volume. Possible values include `unix` (for UNIX mode bits), `ntfs` (for CIFS ACLs), and `mixed` (for mixed NFS and CIFS access). Regardless of the security style, both NFS and CIFS clients can read from and write to the root volume. The unified security style, which applies only to Infinite Volumes, cannot be applied to a Vserver's root volume.

**[-language <Language code>]** - Default Volume Language Code

This optionally specifies the default language encoding setting for the Vserver and its volumes. The default language encoding setting is C.UTF-8, and values with "\*" suffixes are obsolete.

**[-snapshot-policy <snapshot policy>]** - Snapshot Policy

This optionally specifies the Snapshot policy for new volumes created on the Vserver. If no value is specified, the default Snapshot policy is used. You can use the `-snapshot-policy` parameter on the `volume create` or `volume modify` commands to set the Snapshot policy on a specific volume, regardless of its Vserver's Snapshot policy setting.

**[-comment <text>]** - Comment

This optionally specifies a comment for the Vserver.

**[-antivirus-on-access-policy <antivirus policy>]** - Antivirus On-Access Policy

This optionally specifies an antivirus policy for the Vserver. The default value is `default`. This parameter is not supported on a Vserver with Infinite Volume.

**[-quota-policy <text>]** - Quota Policy

This optionally specifies a quota policy for the Vserver. This parameter is not supported on a Vserver with Infinite Volume.

**[-is-repository {true|false}]** - Is Vserver with Infinite Volume

This specifies that the Vserver will contain an Infinite Volume.

## Examples

The following example creates a Vserver named `vs0.example.com`. The Vserver's root volume is named `root_vs0` and is located on aggregate `aggr0`. The Vserver uses NIS for network information, a file for name mapping information, and the default language is U.S. English.

```
cluster::> vsserver create -vsserver vs0.example.com -rootvolume root_vs0 -
aggregate aggr0 -ns-switch nis -nm-switch file
-language en_US
```

## See Also



---

volume create   volume modify

---

## vserver delete

Delete a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver delete` command deletes a specified Vserver. If the Vserver is associated with one or more logical interfaces, one or more volumes (including root and mirror volumes), or one or more volume efficiency policies, you must manually delete them before you can delete the Vserver.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the Vserver that is to be deleted.

### Examples

The following example deletes a Vserver named `vs2.example.com`:

```
cluster::> vserver delete -vserver vs2.example.com
```

## vserver modify

Modify a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver modify` command modifies the attributes of a specified Vserver.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the Vserver that is to be modified.

**[-ns-switch** {nis|file|ldap}, ...] - Name Service Switch

---

This optional parameter specifies the source or sources that are searched for network information and the order in which they are searched. Possible values include nis, file, and ldap. This parameter provides the functionality of the /etc/nsswitch.conf file on UNIX systems; see the UNIX man page for nsswitch.conf(5) for more information.

**[-nm-switch {file|ldap}, ...]** - Name Mapping Switch

This optional parameter specifies the sources that are searched for name mapping information and the order in which they are searched. Possible values include file and ldap.

**[-language <Language code>]** - Default Volume Language Code

This optional parameter specifies the default language encoding setting for the Vserver and its volumes. The default language encoding setting is C.UTF-8, and values with "" suffixes are obsolete. This field is not modifiable on a Vserver with Infinite Volume.

**[-snapshot-policy <snapshot policy>]** - Snapshot Policy

This optional parameter specifies the Snapshot policy for new volumes created on the Vserver. If no value is specified, the default Snapshot policy is used. You can use the `-snapshot-policy` parameter with the `volume create` or `volume modify` commands to set the Snapshot policy on a specific volume, regardless of its Vserver's Snapshot policy setting.

**[-comment <text>]** - Comment

This optional parameter specifies a comment for the Vserver.

**[-antivirus-on-access-policy <antivirus policy>]** - Antivirus On-Access Policy

This optional parameter specifies a default antivirus policy for the Vserver. This value is not modifiable on a Vserver with Infinite Volume.

**[-quota-policy <text>]** - Quota Policy

This optional parameter specifies a quota policy to be used for all volumes associated with a Vserver. You can create and configure multiple, different quota policies, but each Vserver must have one and only one associated quota policy. This parameter is not supported on a Vserver with Infinite Volume.

**[-aggr-list <aggregate name>, ...]** - List of Aggregates Assigned

This optional parameter specifies a confined list of aggregates on which volumes can be created for the Vserver. But these aggregates do not become exclusive property of the Vserver, i.e. they might be assigned for use to other Vservers.

**[-max-volumes <unsigned32\_or\_unlimited>]** - Limit on Maximum Number of Volumes allowed

---

This optional parameter specifies the maximum number of volumes that can be created for the Vserver, including the root volume. This value is not modifiable on a Vserver with Infinite Volume.

**[-admin-state {running|stopped|starting|stopping}]** - Vserver Admin State (privilege: advanced)

Use this parameter to set the admin state of the Vserver if the Vserver start or stop job fails. Possible values include `running` and `stopped`.

**[-allowed-protocols {nfs|cifs|fc|iscsi|ndmp}, ...]** - Allowed Protocols

This optional parameter specifies the list of protocols to be allowed to run on the Vserver. If the values provided here conflict with the ones provided for `disallowed-protocols`, then those values would become part of the `disallowed-protocols`. Possible values include `nfs`, `cifs`, `fc`, and `iscsi`. Possible values for a Vserver with Infinite Volume include `nfs`, and `cifs`.

**[-disallowed-protocols {nfs|cifs|fc|iscsi|ndmp}, ...]** - Disallowed Protocols

This optional parameter specifies the list of protocols to be disallowed to run on the Vserver. If the values provided here conflict with the ones provided for `allowed-protocols`, they would continue to be part of the `disallowed-protocols`. Possible values include `nfs`, `cifs`, `fc`, and `iscsi`. Possible values for a Vserver with Infinite Volume include `nfs`, `cifs`, `fc`, and `iscsi`.

**[-qos-policy-group <text>]** - QoS Policy Group

This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a Vserver, the system will not monitor and control the traffic to it. To remove this Vserver from a policy group, enter the reserved keyword "none". This parameter is not supported on a Vserver with Infinite Volume.

## Examples

The following example specifies a Snapshot policy named `daily`, adds the comment "Sales team access," and modifies the quota policy for a Vserver named `vs0.example.com` to `pol1`.

```
cluster1::> vsserver modify -vsserver vs0.example.com -snapshot-policy daily
               -comment "Sales team access" -quota-policy pol1
```

## See Also

`volume create` `volume modify`

---

## vserver rename

Rename a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver rename` command renames the Vserver.

### Parameters

**-vserver** <text> - Vserver

This specifies the Vserver that is to be renamed.

**-newname** <vserver> - New Vserver name (Use Fully Qualified Domain Name, For example: data.example.com)

This specifies the Vserver's new name. The name must be a unique Vserver name in the cluster. Use a fully qualified domain name (FQDN) - for example, "data.example.com" - for the Vserver name to reduce name collisions in cluster leagues.

### Examples

The following example renames a Vserver named vs1.example.com as vs2.example.com:

```
cluster::> vserver rename -vserver vs1.example.com -newname vs2.example.com
```

## vserver setup

Vserver setup wizard

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command creates and configures a Vserver with storage, network, services, and protocols. You can optionally specify the following parameters for the setup:

- network {true|false}

- 
- storage {true|false}
  - services {ldap|nis|dns}
  - protocols {nfs|cifs|fc|iscsi}

## Parameters

**[-vserver <vserver>]** - Vserver

This optionally specifies the name of the Vserver that is to be created. If a Vserver with the entered name exists, the Vserver is not created, and the wizard will continue with the other configurations.

- Aggregate name

The default value is displayed.

- rootvolume - Root volume name is auto-generated as vs\_root\_vol for a Vserver vs.
- ns-switch and nm-switch - The default value for these fields is file.
- rootvolume-security-style - For CIFS only users, the default value is set to ntfs. Otherwise, the default value is set to unix.
- language - Default volume language code is C.UTF-8.
- snapshot-policy - The default value is default.
- antivirus-on-access-policy - The default value is default.

**[-network [true]]** - Network Setup

This optionally specifies the type of network setup. If you do not enter this parameter, it is set to false. Specify the protocol traffic type as IP or FC.

Note:

IP and FC are case insensitive.

You must enter the following values for IP network interface setup:

- LIF name

The auto-generated LIF name is displayed as the default value.

- Protocol types for the interface - The possible values include nfs, cifs, and iscsi.

---

Note:

iSCSI cannot co-exist with the NFS and CIFS.

- LIF home node

The list of available home nodes is displayed.

- LIF home port

The list of available data ports is displayed.

- IP address
- Network mask
- Role - The default value is data.

You must enter the following values for FCP network interface setup:

- LIF name

The auto-generated LIF name is displayed as the default value.

- LIF home node

The list of available home nodes is displayed.

- LIF home port

The list of available data ports is displayed. You must enter the following value for network route setup:

- Gateway IP address

#### **[-storage [true]] - Storage Setup**

This optionally specifies the Vserver volume setup for a Vserver. If you do not enter this parameter, it is set to false. You must specify the following for Vserver volume setup:

- Volume name

The auto-generated volume name is displayed as a default value.

- Aggregate name

The default aggregate name is displayed.

- 
- Volume size
  - Junction path

The default junction path is displayed as /vol/<vol-name>.

- unix-permissions - The default value is 1777.
- antivirus-on-access-policy - The default policy is default.

**[-services {ldap|nis|dns}, ...]** - Services Setup

This optionally specifies the services setup. Possible values include nis, ldap, and dns. If you do not enter this parameter, it is set to false. You must specify the following for Vserver NIS setup:

- NIS domain name
- IP address of the NIS server

You must specify the following for Vserver LDAP setup:

- LDAP client configuration name
- IP address of LDAP server - The default value is none.
- Port number of the LDAP server - The default value is 389.
- Minimum Bind Authentication Level - The possible values are anonymous, simple, and sasl. The default value is anonymous.
- Bind DN (User)- The default value is none.
- Bind Password
- Base DN - The default value is -.

You must specify the following for Vserver DNS setup:

- DNS domain names
- IP address of the DNS servers

**[-protocols {nfs|cifs|fc|iscsi|ndmp}, ...]** - Configure Data Access protocol

This optionally specifies the protocols setup. Possible values include nfs, cifs, iscsi and fc. If you do not enter this parameter, it is set to false. You must specify the following for Vserver CIFS setup:

- Domain name



- 
- CIFS share name

The default value is /vol/<volume-name>/.

- CIFS share path

The default value is <volume-junction-path>.

- CIFS Access Control List

The default value is No\_Access. You must specify the following for Vserver iSCSI setup:

- igroup name

The auto-generated igroup name is displayed as a default value.

- Initiator names (Comma-separated)

The default value is -.

- Initiator OS - The possible values are solaris, windows, hpux, aix, linux, network, vmware, openvms.

The default value is vmware.

- Volume name to create a LUN
- LUN name

The auto-generated LUN name is displayed as a default value.

- LUN size

You must specify the following for Vserver FCP setup:

- igroup name

The auto-generated igroup name is displayed as a default value.

- WWPN of the initiators (Comma-separated)

The default value is -.

- Initiator OS - The possible values are solaris, windows, hpux, aix, linux, network, vmware, openvms.

The default value is vmware.

- 
- Volume name to create a LUN
  - LUN name

The auto-generated LUN name is displayed as a default value.

- LUN size

## Examples

The following example creates a Vserver named `data.example.com`. After the Vserver `data.example.com` is created, the setup continues with the other sub-wizards such as storage, network, service-configure, and protocol-configure.

```
node::> vservers setup -vservers data.example.com
```

The following example creates a Vserver named `data.example.com`, and configures nis setup, network interface setup, and protocols such as `nfs,cifs`.

```
node::> vservers setup -vservers data.example.com -services nis -network true -  
protocols nfs,cifs
```

## vservers show

Display Vservers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vservers show` command displays the following information:

- Vserver name
- Vserver type ( data, admin, or node - detailed view only)
- Vserver universal unique identifier (detailed view only)
- Root volume name
- Aggregate on which the root volume is located
- Name Service setting
- Name mapping
- Associated NIS domain

- 
- Root volume security style ( unix for UNIX mode bits, ntfs for CIFS ACLs, mixed for both (detailed view only), or unified (Infinite Volumes only))
  - LDAP client
  - Language (detailed view only)
  - Security style of the root volume (detailed view only)
  - Snapshot policy (detailed view only)
  - Comment text (detailed view only)
  - Antivirus on-access policy (detailed view only)
  - Quota policy (detailed view only)
  - Aggregate list (detailed view only)
  - Maximum Volumes (detailed view only)
  - Admin state ( running, stopped, starting, or stopping)
  - Allowed Protocols ( nfs, cifs, fcp, iscsi - detailed view only)
  - Disallowed Protocols ( nfs, cifs, fcp, iscsi - detailed view only)
  - Protocol Services use Data LIFs (detailed view only)
  - Whether the Vserver is a Vserver with Infinite Volume (detailed view only)

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**protocols** ]

If this optional parameter is specified, the command displays the allowed and disallowed set of protocols for the Vserver(s).

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver>] - Vserver

If this parameter is specified, the command displays detailed information about the specified Vserver.

---

**[-type <vserver type>]** - Vserver Type

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified Vserver type. Types include admin for the cluster-wide management Vserver, data for a standard Vserver, and node for a single node in the cluster.

**[-uuid <UUID>]** - Vserver UUID

If this parameter is specified, the command displays information only about the Vserver that match the specified UUID.

**[-rootvolume <volume name>]** - Root Volume

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified root volume.

**[-aggregate <aggregate name>]** - Aggregate

If this parameter is specified, the command displays information only about the Vserver or Vservers that have their root volumes contained by the specified aggregate.

**[-ns-switch {nis|file|ldap}, ...]** - Name Service Switch

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified Name Service Switch setting.

**[-nm-switch {file|ldap}, ...]** - Name Mapping Switch

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified name mapping switch setting.

**[-nisdomain <nis domain>]** - NIS Domain

If this parameter is specified, the command displays information only about the Vserver or Vservers that use the specified NIS domain.

**[-rootvolume-security-style {unix|ntfs|mixed|unified}]** - Root Volume Security Style

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified root-volume security style. The unified security style, which applies only to Infinite Volumes, cannot be applied to a Vserver's root volume.

**[-ldap-client <text>]** - LDAP Client

If this parameter is specified, the command displays information only about the Vserver or Vservers that use the specified LDAP client.

**[-language <Language code>]** - Default Volume Language Code

---

If this parameter is specified, the command displays information only about the Vserver or Vservers that use the specified language. To determine the available languages, enter "vserver show -language ?" at the clustershell command prompt.

**[-snapshot-policy <snapshot policy>]** - Snapshot Policy

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified Snapshot policy.

**[-comment <text>]** - Comment

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified comment.

**[-antivirus-on-access-policy <antivirus policy>]** - Antivirus On-Access Policy

If this parameter is specified, the command displays information only about the Vserver or Vservers that use the specified antivirus policy.

**[-quota-policy <text>]** - Quota Policy

If this parameter is specified, the command displays information only about the Vserver or Vservers that use the specified quota policy.

**[-aggr-list <aggregate name>, ...]** - List of Aggregates Assigned

If this parameter is specified, the command displays information only about the Vserver or Vservers to which the specified aggregate(s) are assigned for use.

**[-max-volumes <unsigned32\_or\_unlimited>]** - Limit on Maximum Number of Volumes allowed

If this parameter is specified, the command displays information only about the Vserver or Vservers on which the specified maximum volume count is configured.

**[-admin-state {running|stopped|starting|stopping}]** - Vserver Admin State (privilege: advanced)

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified admin-state.

**[-allowed-protocols {nfs|cifs|fcpl|iscsi|ndmp}, ...]** - Allowed Protocols

If this parameter is specified, the command displays information only about the Vserver or Vservers on which the specified protocols are allowed to run.

**[-disallowed-protocols {nfs|cifs|fcpl|iscsi|ndmp}, ...]** - Disallowed Protocols

If this parameter is specified, the command displays information only about the Vserver or Vservers on which the specified protocols are disallowed to run.

**[-is-repository {true|false}]** - Is Vserver with Infinite Volume

---

If this parameter is specified, the command displays information only about the Vservers which have the specified is-repository value. This will be true for Vservers with Infinite Volumes.

**[-qos-policy-group <text>] - QoS Policy Group**

Display the Vservers that match the specified qos-policy-group.

A policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a Vserver, the system will not monitor and control the traffic to it.

**Examples**

The following example displays information about all Vservers.

```
cluster::> vserver show
Vserver      Type      Admin      Root      Aggregate  Name      Name
-----      -
node1        node      -          -          -          -          -
node2        node      -          -          -          -          -
cluster      admin    -          -          -          -          -
vs1.example.com
  data      stopped  -          -          -          file      file
vs2.example.com
  data      running  vs2_root  abc        file      file
5 entries were displayed.
```

---

## vserver start

Start a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver start` command starts data access on a Vserver.

### Parameters

**-vserver** <vserver> - Vserver

This specifies the name of the Vserver on which data access is to be started.

Note:

The name must be 47 characters or less.

**[-foreground {true|false}]** - Foreground Process

This specifies if the `vserver start` command should be executed in the foreground or background. If you do not enter this parameter, it is set to true, and the `vserver start` command is executed in the foreground.

### Examples

The following example starts data access on Vserver `vs0.example.com` in the background.

```
cluster::> vserver start -vserver vs0.example.com -foreground false
```

## vserver stop

Stop a Vserver

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver stop` command stops data access on a Vserver.

---

## Parameters

**-vserver** <vserver> - Vserver

This specifies the name of the Vserver on which data access is to be stopped.

Note:

The name must be 47 characters or less.

**[-foreground {true|false}]** - Foreground Process

This specifies if `vserver stop` command should be executed in the foreground or background. If you do not enter this parameter, it is set to true, and the `vserver stop` command is executed in the foreground.

## Examples

The following example stops data access on Vserver `vs0.example.com` in the background.

```
cluster::> vserver stop -vserver vs0.example.com -foreground false
```

## vserver audit create

Create an audit configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver audit create` command creates an audit configuration for a Vserver.

When you create an audit configuration, you can also specify the rotation method. By default, the audit log is rotated based on size.

You can use the time-based rotation parameters in any combination (`-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute`). The `-rotate-schedule-minute` parameter is mandatory. All other time-based rotation parameters are optional.

The rotation schedule is calculated by using all the time-related values. For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all



---

months of the year. If you specify only one or two time-based rotation parameters (say `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months. For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30.

If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently. For example if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13 then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

This command is not supported on a Vserver with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which to create the audit configuration. The Vserver must already exist.

**-destination** <text> - Log Destination Path

This parameter specifies the audit log destination path, where consolidated audit logs are stored. If the path is not valid, the command fails.

**[ -rotate-size** {<integer>[KB|MB|GB|TB|PB]] - Log File Size Limit

This parameter specifies the audit log file size limit. By default, the audit log is rotated based on size. The default audit log size is 100 MB.

**[ -rotate-schedule-month** <cron\_month>, ...] - Log Rotation Schedule: Month

This parameter specifies the monthly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated during the months January, March, and August, or during all the months. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, and all. Specify "all" to rotate the audit logs every month.

**[ -rotate-schedule-dayofweek** <cron\_dayofweek>, ...] - Log Rotation Schedule: Day of Week

This parameter specifies the daily (day of the week) schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and all. Specify "all" to rotate the audit logs every day.

---

**[-rotate-schedule-day <cron\_dayofmonth>, ...] - Log Rotation Schedule: Day**

This parameter specifies the day of the month schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month. Valid values range from 1 to 31. Specify "all" to rotate the audit logs every day of the month.

**[-rotate-schedule-hour <cron\_hour>, ...] - Log Rotation Schedule: Hour**

This parameter specifies the hourly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at 6 a.m and 10 a.m. Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specify "all" to rotate the audit logs every hour.

**-rotate-schedule-minute <cron\_minute>, ... } - Log Rotation Schedule: Minute**

This parameter specifies the minute schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at the 30th minute. Valid values range from 0 to 59. Specify "all" to rotate the audit logs every minute.

**[-rotate-limit <integer>] - Log Files Rotation Limit**

This parameter specifies the audit log files rotation limit. A value of 0 indicates that all the log files are retained. The default value is 0. For example, if you enter a value of 5, the last five audit logs are retained.

## Examples

The following examples create an audit configuration for Vserver vs1 using size-based rotation.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-size 10MB -rotate-limit 5
```

The following example creates an audit configuration for Vserver vs1 using time-based rotation. The audit logs are rotated monthly, all days of the week, at 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30
```

The following example creates an audit configuration for Vserver vs1 using time-based rotation. The audit logs are rotated in January, March, May, July, September, and November on Monday, Wednesday, and Friday, at 6:15, 6:30, 6:45, 12:15, 12:30, 12:45, 18:15, 18:30, and 18:45. The last 6 audit logs are retained.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-schedule-month January,March,May,July,September,November -rotate-schedule-dayofweek Monday,Wednesday,Friday -rotate-schedule-hour 6,12,18 -rotate-schedule-minute 15,30,45 -rotate-limit 6
```

---

## vserver audit delete

Delete audit configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver audit delete` command deletes the audit configuration for a Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver associated with the audit configuration to be deleted.

**[-force [true]]** - Force Delete (privilege: advanced)

This parameter is used to forcibly delete the audit configuration. By default the setting is `false`.

### Examples

The following example deletes the audit configuration for Vserver vs1.

```
cluster1::> vserver audit delete -vserver vs1
```

## vserver audit disable

Disable auditing

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver audit disable` command disables auditing for a Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

---

This parameter specifies the name of the Vserver for which auditing is to be disabled. The Vserver audit configuration must already exist.

## Examples

The following example disables auditing for Vserver vs1.

```
cluster1::> vserver audit disable -vserver vs1
```

## vserver audit enable

Enable auditing

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver audit enable` command enables auditing for a Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver for which auditing is to be enabled. The Vserver audit configuration must already exist.

**[-force [true]]** - Force Enable (privilege: advanced)

This parameter is used to forcibly enable auditing. By default the setting is `false`.

## Examples

The following example enables auditing for Vserver vs1.

```
cluster1::> vserver audit enable -vserver vs1
```

## vserver audit modify

Modify the audit configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

---

The `vserver audit modify` command modifies an audit configuration for a Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver for which the audit configuration is to be modified. The Vserver audit configuration must already exist.

If you have configured time-based rotation, modifying one parameter of time-based rotation schedule does not affect the other parameters. For example, if the rotation schedule is set to run at Monday 12:30 a.m., and you modify the `-rotate-schedule-dayofweek` parameter to Monday,Wednesday,Friday, the new rotation-schedule rotates the audit logs on Monday, Wednesday, and Friday at 12:30 a.m. To clear time-based rotation parameters, you must explicitly set that portion to "-". Some time-based parameters can also be set to "all".

**[-destination <text>]** - Log Destination Path

This parameter specifies the audit log destination path, where consolidated audit logs are stored. If the path is not valid, command fails.

**{ [-rotate-size {<integer>[KB|MB|GB|TB|PB]}]}** - Log File Size Limit

This parameter specifies the audit log file size limit. By default, the audit log is rotated based on size. The default audit log size is 100 MB.

**| [-rotate-schedule-month <cron\_month>, ...]** - Log Rotation Schedule: Month

This parameter specifies the monthly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated during the months January, March, and August, or during all the months. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, and all. Specify "all" to rotate the audit logs every month.

**[-rotate-schedule-dayofweek <cron\_dayofweek>, ...]** - Log Rotation Schedule: Day of Week

This parameter specifies the daily (day of the week) schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and all. Specify "all" to rotate the audit logs every day.

**[-rotate-schedule-day <cron\_dayofmonth>, ...]** - Log Rotation Schedule: Day

This parameter specifies the day of the month schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month. Valid values range from 1 to 31.

---

**[-rotate-schedule-hour <cron\_hour>, ...]** - Log Rotation Schedule: Hour

This parameter specifies the hourly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at 6 a.m and 10 a.m. Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specify "all" to rotate the audit logs every hour.

**[-rotate-schedule-minute <cron\_minute>, ...]** } - Log Rotation Schedule: Minute

This parameter specifies the minute schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at the 30th minute. Valid values range from 0 to 59.

**[-rotate-limit <integer>]** - Log Files Rotation Limit

This parameter specifies the audit log files rotation limit. A value of 0 indicates that all the log files are retained. The default value is 0.

## Examples

The following example modifies the rotate-size and rotate-limit field for Vserver vs1.

```
cluster1::> vserver audit modify -vserver vs1 -rotate-size 10MB -rotate-limit 3
```

The following example modifies an audit configuration for Vserver vs1 using the time-based rotation method. The audit logs are rotated monthly, all days of the week, at 12:30.

```
cluster1::> vserver audit modify -vserver vs1 -destination /audit_log -rotate-  
schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -  
rotate-schedule-minute 30
```

---

## vserver audit show

Display the audit configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver audit show` command displays audit configuration information about Vservers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all the Vservers:

- Vserver name
- Audit state
- Target directory

You can specify the `-fields` parameter to specify which audit configuration information to display about Vservers.

You can specify additional parameters to display only information that matches those parameters. For instance, to display information about the log file rotation size of a Vserver whose value matches 10 MB, run the command with the `-rotate-size 10MB` parameter.

You can specify the `-instance` parameter to display audit configuration information for all Vservers in list form.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-log-save-details ]**

You can specify the `-log-save-details` parameter to display the following information about all the Vservers:

- Vserver name
- Rotation file size

- 
- Rotation schedules
  - Rotation limit

| **[-instance ]** }

If you specify the **-instance** parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information about the specified Vserver.

**[-state {true|false}]** - Auditing State

If you specify this parameter, the command displays information about the Vservers that use the specified audit state value.

**[-destination <text>]** - Log Destination Path

If you specify this parameter, the command displays information about the Vservers that use the specified destination path.

**[-rotate-size {<integer>[KB|MB|GB|TB|PB]}]** - Log File Size Limit

If you specify this parameter, the command displays information about the Vservers that use the specified log file rotation size.

**[-rotate-schedule-month <cron\_month>, ...]** - Log Rotation Schedule: Month

If you specify this parameter, the command displays information about the Vservers that use the specified month of the time-based log rotation scheme. Valid values are January, February, March, April, May, June, July, August, September, October, November, and December.

**[-rotate-schedule-dayofweek <cron\_dayofweek>, ...]** - Log Rotation Schedule: Day of Week

If you specify this parameter, the command displays information about the Vservers that use the specified day of the week of the time-based log rotation scheme. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.

**[-rotate-schedule-day <cron\_dayofmonth>, ...]** - Log Rotation Schedule: Day

If you specify this parameter, the command displays information about the Vservers that use the specified day of the month of the time-based log rotation scheme. Valid values range from 1 to 31.

**[-rotate-schedule-hour <cron\_hour>, ...]** - Log Rotation Schedule: Hour



---

If you specify this parameter, the command displays information about the Vservers that use the specified hour of the time-based log rotation scheme. Valid values range from 0 (midnight) to 23 (11:00 p.m.).

**[-rotate-schedule-minute <cron\_minute>, ...]** - Log Rotation Schedule: Minute

If you specify this parameter, the command displays information about the Vservers that use the specified minute of the time-based log rotation scheme. Valid values range from 0 to 59.

**[-rotate-schedule-description <text>]** - Rotation Schedules

If you specify this parameter, the command displays information about the Vservers that use the specified rotation schedules. This field is derived from the rotate-time fields.

**[-rotate-limit <integer>]** - Log Files Rotation Limit

If you specify this parameter, the command displays information about the Vservers that use the specified rotation limit value.

## Examples

The following example displays the name, audit state, and target directory for all Vservers.

```
cluster1::> vserver audit show
Vserver      State  Target Directory
-----
vsl          false  /audit_log
```

The following example displays the vserver names and details about the audit log for all Vservers.

```
cluster1::> vserver audit show -log-save-details
Vserver      Rotation File Size Rotation Schedule Rotation Limit
-----
vsl          100MB      -                  0
```

The following example displays in list form all audit configuration information about all Vservers.

```
cluster1::> vserver audit show -instance
Vserver: vsl
Auditing state: true
Log Destination Path: /audit_log
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

---

## vserver cifs create

Create a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs create` command creates a CIFS server on a Vserver. When you create the CIFS server, you must add it to an existing CIFS domain. When you enter this command, the storage system prompts you to provide the credentials of a user account that has sufficient privileges to add computers to the `-ou` container within the `-domain` domain. The user account must have a password that cannot be empty.

Note:

Each Vserver can have only one CIFS server.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which to create the CIFS server. The Vserver must already exist.

**-cifs-server** <NetBIOS> - CIFS Server NetBIOS Name

This parameter specifies the name of the CIFS server (up to 15 characters).

**-domain** <TextNoCase> - Fully Qualified Domain Name

This parameter specifies the name of the Active Directory domain to associate with the CIFS server.

**[-ou <text>]** - Organizational Unit

This parameter specifies the organizational unit within the Active Directory domain to associate with the CIFS server. By default, this parameter is set to CN=Computers.

**[-default-site <text>]** - Default Site Used by LIFs Without Site Membership

This parameter specifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site.

**[-status-admin {down|up}]** - CIFS Server Administrative Status

---

Use this parameter to specify whether the initial administrative status of the cifs server is up or down. The default setting is up.

## Examples

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and domain EXAMPLE.com.

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1 -domain  
EXAMPLE.com
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "EXAMPLE.com" domain.

Enter the user name: Administrator

Enter the password:

---

## vserver cifs delete

Delete a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs delete` command deletes a CIFS server.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for the CIFS server you want to delete.

### Examples

The following example deletes the CIFS server from a Vserver named vs1:

```
cluster1::> vserver cifs delete -vserver vs1
```

## vserver cifs modify

Modify a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs modify` command modifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for the CIFS server whose associated site you want to modify.

**[-domain <TextNoCase>]** - Fully Qualified Domain Name

---

This parameter specifies the fully qualified name of the Active Directory domain to associate with the CIFS server.

**[-default-site <text>]** - Default Site Used by LIFs Without Site Membership

This parameter specifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site.

**[-status-admin {down|up}]** - CIFS Server Administrative Status

Use this parameter to modify the administrative status of the cifs server. Modify the administrator status to `down` to stop cifs access.

## Examples

The following example changes the default site and administrative status of the CIFS server associated with Vserver "vs1":

```
cluster1::> vserver cifs modify -vserver vs1 -default-site default -status-admin up
```

The following example modifies the Active Directory domain for the CIFS server associated with Vserver "vs1". The administrative status of the CIFS server must be set to "down" in order to proceed with Active Directory domain modification. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status-admin down
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: administrator

Enter the password:

```
cluster1::>
```

---

## vserver cifs nbtstat

Display NetBIOS information over TCP connection

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs nbtstat` command displays information about NetBIOS over TCP (NBT) connections for the cluster. It displays the IP address associated with the interfaces, the IP addresses of the WINS servers in use, and information about the registered NetBIOS names for the cluster. You can use this command to troubleshoot NetBIOS name resolution problems.

Note:

NetBIOS name service (NBNS) over IPv6 is not supported.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**node** {<nodename>|local}] - Node

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified node.

[-**vserver** <vserver name>] - Vserver

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified Vserver.

[-**nbt-name** <text>] - NBT Name

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name.

---

**[-netbios-suffix <Hex String>]** - NetBIOS Suffix

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS suffix.

**[-interface <IP Address>, ...]** - Interfaces

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified IP address.

**[-wins-servers <IP Address>, ...]** - Servers

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified WINS servers.

**[-server-state <text>, ...]** - Server State (active, inactive)

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified WINS server state. The following are possible values for this parameter:

- active
- inactive

**[-nbt-scope <text>]** - NBT Scope

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name scope.

**[-nbt-mode <text>]** - NBT Mode

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name service mode. The following are possible values for this parameter:

- 'p' - Point to Point
- 'h' - Hybrid
- 'm' - Mixed
- 'b' - Broadcast

**[-state <text>]** - State

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name registration state. The following are possible values for this parameter:

- must\_register

- must\_unregister
- wins
- broadcast
- name\_released
- wins\_conflict
- broadcast\_conflict

**[-time-left <integer>]** - Time Left

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified registration time left in minutes with the WINS server.

**[-type <text>]** - Type

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified name registration type. The following are possible values for this parameter:

- registered
- active
- permanent
- group

## Examples

The following example displays the NetBIOS name service information.

```
cluster1::> nbtstat
(vserver cifs nbtstat)

Vserver: vs1
Node: cluster1-01
Interfaces:
  10.10.10.32
  10.10.10.33
Servers: 17.17.1.2 (active )
NBT Scope: [ ]
NBT Mode: [h]
NBT Name NetBIOS Suffix State Time Left Type
-----
CLUSTER_1 00 wins 57
CLUSTER_1 20 wins 57

Vserver: vs1
Node: cluster1-02
Interfaces:
  10.10.10.35
Servers: 17.17.1.2 (active )
CLUSTER_1 00 wins 58
```



---

CLUSTER_1	20	wins	58
4 entries were displayed.			

---

## vserver cifs password-change

Change the domain account password for a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs password-change` changes the domain account password for a CIFS server.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver for whose CIFS server you want to change the domain account password.

### Examples

The following example changes the password for the CIFS server on a Vserver named `vs1`.

```
cluster1::> vserver cifs password-change -vserver vs1
cluster1::>
```

## vserver cifs password-reset

Reset the domain account password for a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs password-reset` command resets the domain account password for a CIFS server. This may be required if the password stored along with the machine account in the Windows Active Directory domain is changed or reset without the Vserver's knowledge. The operation requires the credentials for a user with permission to reset the password in the organizational unit (OU) that the machine account is a member of.

---

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver for whose CIFS server you want to reset the domain account password.

## Examples

The following example resets the password for the CIFS server on a Vserver named vs1.

```
cluster1::> vserver cifs password-reset -vserver vs1
Enter your user ID: Administrator
Enter your password:
cluster1::>
```

## vserver cifs show

Display CIFS servers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs show` command displays information about CIFS servers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

- Vserver name
- CIFS server NetBIOS name
- Domain or workgroup name
- Authentication style

You can specify the `-fields` parameter to specify which fields of information to display about CIFS servers. In addition to the fields above, you can display the following fields:

- Default site
- Fully-qualified domain name

---

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about CIFS servers that are in the CIFS domain named RUBY, run the command with the `-domain-workgroup RUBY` parameter.

You can specify the `-instance` parameter to display all information for all CIFS servers in list form.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vsriver <vsriver name>]** - Vserver

If you specify this parameter, the command displays information only about the CIFS servers for the specified Vserver.

**[-cifs-server <NetBIOS>]** - CIFS Server NetBIOS Name

If you specify this parameter, the command displays information only for CIFS servers that match the specified NetBIOS CIFS server name.

**[-domain-workgroup <CIFS domain>]** - NetBIOS Domain/Workgroup Name

If you specify this parameter, the command displays information only for CIFS servers that are in the specified NetBIOS domain or workgroup.

Note:

Workgroups are not supported in this release.

**[-domain <TextNoCase>]** - Fully Qualified Domain Name

If you specify this parameter, the command displays information only for CIFS servers that are in the specified domain.

**[-default-site <text>]** - Default Site Used by LIFs Without Site Membership

If you specify this parameter, the command displays information only for CIFS servers that have the specified default site.

**[-auth-style {domain|workgroup}]** - Authentication Style

---

If you specify this parameter, the command displays information only for CIFS servers that match the specified authentication style.

Note:

Workgroups are not supported in this release, so the only possible authentication style is `domain`.

**`[-status-admin {down|up}]` - CIFS Server Administrative Status**

If you specify this parameter, the command displays information only for CIFS servers that match the specified administrative status.

**Examples**

The following example displays a subset of the information about all CIFS servers.

```
cluster1::> vserver cifs show
```

Vserver	Server Name	Domain/Workgroup Name	Authentication Style
vs1	CIFSSERVER1	EXAMPLE	domain

The following example displays all information about all CIFS-enabled Vservers in list form.

```
cluster1::> vserver cifs show -instance
```

Vserver: vs1

CIFS Server NetBIOS Name: CIFSSERVER1

NetBIOS Domain/Workgroup Name: EXAMPLE

Fully Qualified Domain Name: EXAMPLE.COM

Default Site Used by LIFs Without Site Membership:

Authentication Style: domain

CIFS Server Administrative Status: up

---

## vserver cifs start

Start a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command starts the CIFS server on the specified Vserver. The CIFS server must already exist. To create a CIFS server, run `vserver cifs create`.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies a Vserver containing a configured CIFS server that has been stopped.

### Examples

The following example starts the CIFS server on Vserver vs1:

```
cluster1::> cifs start -vserver vs1
```

### See Also

`vserver cifs create`

---

## vserver cifs stop

Stop a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command stops the CIFS server on the specified Vserver.

Note:

Established sessions will be terminated and their open files closed. Workstations with cached data will not be able to save those changes, which could result in data loss.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies a Vserver containing a configured CIFS server that is running.

### Examples

The following example stops the CIFS server on Vserver vs1:

```
cluster1::> cifs stop -vserver vs1
```

## vserver cifs branchcache create

Create the CIFS BranchCache service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs branchcache create` command creates the configuration for computing and retrieving BranchCache hash data. Only a single instance of the BranchCache service can be created on a Vserver.

The `vserver cifs branchcache create` command is not supported for Vservers with Infinite Volume.

---

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver on which you want to set up the BranchCache service.

**[-versions** {v1-enable|v2-enable|enable-all}, ...] - Supported BranchCache Versions

This optional parameter specifies a list of versions of the BranchCache protocol that the storage system supports. The default is `enable-all`. This list can include one or more of the following:

- v1-enable - This option enables BranchCache Version 1.
- v2-enable - This option enables BranchCache Version 2.
- enable-all - This option enables all supported versions of BranchCache.

**-hash-store-path** <text> - Path to Hash Store

This parameter specifies an existing directory into which the hash data is stored. Read-only paths, such as snapshot directories, are not allowed.

**[-hash-store-max-size** {<integer>[KB|MB|GB|TB|PB]]} - Maximum Size of the Hash Store

This optional parameter specifies the maximum size to use for the hash data. If the size of the hash data exceeds this value, older hashes are deleted to make room for newer hashes. The default is 1 GB.

**[-server-key** <text>] - Encryption Key Used to Secure the Hashes

This optional parameter specifies a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server.

**[-operating-mode** <BranchCache Mode>] - CIFS BranchCache Operating Modes

This optional parameter specifies the mode in which the BranchCache service operates. The default is `per-share`. Possible values include:

- disable - This option disables the BranchCache service for the Vserver.
- all-shares - This option enables the BranchCache service for all the shares on this Vserver.
- per-share - This option enables the BranchCache service on a per-share basis. You can enable the BranchCache service on an existing share by adding the



---

branchcache flag in the `-share-properties` parameter of the `vserver cifs share modify` command.

## Examples

The following example creates the BranchCache service on the Vserver named `vs1`. The path to the hash store is `/vs1_hash_store`.

```
cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /vs1_hash_store
```

The following example creates the BranchCache service on the Vserver `vs1`. The path to the hash store is `/vs_hash_store`. The service is enabled on all the shares of the Vserver, supports BranchCache version 2, supports a maximum of 1 GB of BranchCache hashes, and secures the hashes using the key "vs1 secret".

```
cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /vs1_hash_store -operating-mode all-shares -versions v2-enable -hash-store-max-size 1GB -server-key "vs1 secret"
```

## See Also

`vserver cifs share modify`

---

## vserver cifs branchcache delete

Stop and remove the CIFS BranchCache service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs branchcache delete` command stops and removes the Vserver BranchCache configuration.

The `vserver cifs branchcache delete` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver whose BranchCache configuration you want to remove.

**-flush-hashes** {true|false} - Delete Existing Hashes

This parameter specifies whether to keep or delete all existing hashes after deleting the BranchCache service.

### Examples

The following example stops and removes the BranchCache service on the Vserver vs1. It also deletes all existing hashes.

```
cluster1::> vserver cifs branchcache delete -flush-hashes true -vserver vs1
```

## vserver cifs branchcache hash-create

Force CIFS BranchCache hash generation for the specified path or file

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

---

The `vserver cifs branchcache hash-create` command causes the BranchCache service to compute hashes for a single file, for a directory, or for all the files in a directory structure if you specify the `-recurse` option.

The `vserver cifs branchcache hash-create` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver on which the hash is computed.

**-path** <text> - Path of File or Directory to Hash

This parameter specifies the path of the directory or file for which hashes are to be computed. If a file is specified, the hashes are computed on the whole file. If a directory is specified, hashes are computed on all files within the directory.

**-recurse** {true|false} - Process All Files in the Directory Recursively

If this option is set to true and the `-path` parameter specifies a directory, hashes are computed recursively for all directories in the path.

## Examples

The following example creates hashes for the file "report.doc":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /repository/  
report.doc -recurse false
```

The following example creates hashes for all the files in the directory "repository":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /repository -  
recurse false
```

The following example recursively creates hashes for all the files and directories inside the directory "documents":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /documents -  
recurse true
```

## vserver cifs branchcache hash-flush

Flush all generated BranchCache hashes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver cifs branchcache hash-flush` command deletes all hash data from the configured hash store.

The `vserver cifs branchcache hash-flush` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver whose hash data is to be deleted.

## Examples

The following example flushes all the hashes for Vserver vs1:

```
cluster1::> vserver cifs branchcache hash-flush -vserver vs1
```

## vserver cifs branchcache modify

Modify the CIFS BranchCache service settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache modify` command modifies the configuration for computing and retrieving BranchCache hash data.

The `vserver cifs branchcache modify` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver whose BranchCache service is to be modified.

**[-versions {v1-enable|v2-enable|enable-all}, ...]** - Supported BranchCache Versions

---

This optional parameter specifies a list of versions of the BranchCache protocol that the storage system supports. The default is `enable-all`. This list can include one or more of the following:

- `v1-enable` - This option enables BranchCache Version 1.
- `v2-enable` - This option enables BranchCache Version 2.
- `enable-all` - This option enables all supported versions of BranchCache.

**`[-operating-mode <BranchCache Mode>]`** - CIFS BranchCache Operating Modes

This optional parameter specifies the mode in which the BranchCache service operates. The default is `per-share`. Possible values include:

- `disable` - This option disables the BranchCache service for the Vserver.
- `all-shares` - This option enables the BranchCache service for all the shares on this Vserver.
- `per-share` - This option enables the BranchCache service on a per-share basis. You can enable the BranchCache service on an existing share by adding the `branchcache` flag in the `-share-properties` parameter of the `vserver cifs share modify` command.

**`[-hash-store-max-size {<integer>[KB|MB|GB|TB|PB]}]`** - Maximum Size of the Hash Store

This optional parameter specifies the maximum size to use for the hash data. If the size of the hash data exceeds this value, older hashes are deleted to make room for newer hashes. The default is 1 GB.

**`[-flush-hashes {true|false}]`** - Delete Existing Hashes

This parameter specifies whether to keep or delete all the existing hashes. This must be set to `true` when modifying the server key.

**`[-hash-store-path <text>]`** - Path to Hash Store

This parameter specifies an existing directory into which the hash data is stored. Read-only paths, such as snapshot directories, are not allowed.

**`[-server-key <text>]`** - Encryption Key Used to Secure the Hashes

This optional parameter specifies a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you specify this parameter, all existing hashes for the Vserver are deleted.

## Examples

---

The following example modifies the BranchCache service on the Vserver named vs1. The path to the hash store is /vs1\_hash\_store\_2, the server key used to secure the hashes is set to "new vs1 secret", all existing hashes are removed, the service supports all BranchCache versions, and is enabled on a per-share basis.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -hash-store-path /  
vs1_hash_store_2 -server-key "new vs1 secret" -flush-hashes true -versions  
enable-all -operating-mode per-share
```

The following example modifies the BranchCache service on the Vserver vs1. The service is enabled on all the shares of the Vserver, supports BranchCache version 1, and supports a maximum of 1 TB of BranchCache hashes.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode all-  
shares -versions v1-enable -hash-store-max-size 1TB
```

## See Also

[vserver cifs share modify](#)

---

## vserver cifs branchcache show

Display the CIFS BranchCache service status and settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs branchcache show` command displays information about the BranchCache configuration for the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information:

- Operating Mode
- Allowed Versions
- Maximum Size
- Path

You can specify additional parameters to display only information that matches those parameters.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>`, ... parameter, the command displays only the fields that you specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

[-**vserver** <vserver name>] - Vserver

If you specify this parameter, the command displays information for the specified Vserver.

[-**versions** {v1-enable|v2-enable|enable-all}, ...] - Supported BranchCache Versions

If you specify this parameter, the command displays information for the Vservers that support the specified BranchCache versions.

---

**[-hash-store-path <text>]** - Path to Hash Store

If you specify this parameter, the command displays information for Vservers that store their hashes at the specified location.

**[-hash-store-max-size {<integer>[KB|MB|GB|TB|PB]}]** - Maximum Size of the Hash Store

If you specify this parameter, the command displays information for Vservers that have a maximum hash store size that is set to the specified value.

**[-server-key <text>]** - Encryption Key Used to Secure the Hashes

If you specify this parameter, the command displays information for Vservers that have the specified server key.

**[-operating-mode <BranchCache Mode>]** - CIFS BranchCache Operating Modes

If you specify this parameter, the command displays information for Vservers whose BranchCache configuration operates in the specified mode.

## Examples

The following example displays a subset of the information about the BranchCache service in the cluster.

```
cluster1::> vserver cifs branchcache show
Vserver      Operating  Allowed  Max    Path
-----
vs1          per_share enable_all 1GB    /hash_dir/
```

The following example displays all information about all the Vservers with BranchCache configurations.

```
cluster1::> vserver cifs show -instance
Vserver: vs1
Supported Versions of BranchCache: enable_all
Path to Hash Store: /hash_dir/
Maximum Size of the Hash Store: 1GB
Encryption Key Used to Secure the Hashes: asdad
CIFS BranchCache Operating Modes: per_share
```

The following example displays information about BranchCache configurations that store the hash data at the location /branchcache\_hash\_store.

```
cluster1::> vserver cifs branchcache show -hash-store-path /
branchcache_hash_store
Vserver      Operating  Allowed  Max    Path
-----
vs1          per_share enable_all 1GB    /branchcache_hash_store
```



---

## vserver cifs domain discovered-servers reset-servers

Reset and rediscover servers for a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain discovered-servers reset-servers` command discards information the storage system has stored about domain controllers, LDAP, and NIS servers. After that, it begins the discovery process to reacquire current information about external servers.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

### Examples

The following is an example use of this command. It produces no output.

```
cluster1::> vserver cifs domain discovered-servers reset-servers
cluster1::>
```

## vserver cifs domain discovered-servers show

Display discovered server information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain discovered-servers show` command displays information about the discovered servers for the CIFS domains of one or more Vservers. Server displays are grouped by node and Vserver, and each group is preceded by the

---

node and Vserver identification. Within each grouping, the server display is limited to those associated with the domain specified by the domain parameter, if it is present.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node <nodename>|local]** - Node

If you use this parameter, the command only displays servers for the specified node.

**[-vserver <vserver name>]** - Vserver

If you use this parameter, the command only displays servers for the specified Vserver.

**[-domain <TextNoCase>]** - Fully Qualified Domain Name

If you use this parameter, the command only displays servers in the specified domain.

**[-type {Unknown|KERBEROS|MS-LDAP|MS-DC|LDAP|NIS}]** - Server Type

If you use this parameter, the command only displays servers of the specified type.

**[-name <text>]** - Server Name

If you use this parameter, the command only displays servers the with the specified name. This can result in multiple lines because the same server may provide multiple services.

**[-preference {unknown|preferred|favored|adequate}]** - Preference

If you use this parameter, the command only displays servers of the specified preference level.

**[-address <InetAddress>]** - Server Address

If you use this parameter, the command only displays servers with the specified IP address. This can result in multiple lines because the same server may provide multiple services.

**[-status {OK|unavailable|slow|expired}]** - Status

If you use this parameter, the command only displays servers of the specified status.

---

# Examples

The following example display shows the information provided by this command.

```
cluster1::> vserver cifs domain discovered-servers show
Node: node1
Vserver: vs1
Domain Name      Type      Preference DC-Name      DC-Address      Status
-----
" "              NIS       preferred  192.168.10.222 192.168.10.222 OK
example.com      MS-LDAP   adequate  DC-1          192.168.192.24 OK
example.com      MS-LDAP   adequate  DC-2          192.168.192.25 OK
example.com      MS-DC     adequate  DC-1          192.168.192.24 OK
example.com      MS-DC     adequate  DC-2          192.168.192.25 OK
5 entries were displayed.
```

---

## vserver cifs domain preferred-dc add

Add to a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain preferred-dc add` command adds one or more domain controllers to be used in preference to all others by the specified Vserver for interactions with the specified domain. If a list already exists for the specified domain, the new list is merged with the existing list.

Note:

Each Vserver discovers domain controllers and attempts to sort them internally based on real-world performance. Therefore it should not be necessary to create a preferred list of domain controllers under most circumstances.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver for which you want to add preferred domain controllers.

**-domain** <TextNoCase> - Fully Qualified Domain Name

This parameter specifies the fully-qualified name of the domain that the domain controllers belong to.

**-preferred-dc** <InetAddress>, ... - Preferred Domain Controllers

This parameter specifies a comma-delimited list of IP addresses for domain controllers that belong to the domain specified in the `-domain` parameter.

### Examples

The following example adds two domain controllers (192.168.0.100 and 192.168.0.101) to the preferred list used by Vserver vs1 when connecting to the example.com domain:

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain example.com  
-preferred-dc 192.168.0.100,192.168.0.101
```

---

## vserver cifs domain preferred-dc remove

Remove from a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain preferred-dc remove` command removes one or more domain controllers from the list used by the specified Vserver for interactions with the specified domain. If a list of preferred domain controllers is not provided, the entire list for the specified domain is removed.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to remove preferred domain controllers.

**-domain** <TextNoCase> - Fully Qualified Domain Name

This parameter specifies the fully-qualified name of the domain that the domain controllers belong to.

**[-preferred-dc** <InetAddress>, ...] - Preferred Domain Controllers

This parameter specifies a comma-delimited list of IP addresses for domain controllers that belong to the domain specified in the `-domain` parameter.

### Examples

The following example removes one domain controller (192.168.0.101) from the preferred list used by Vserver vs1 when connecting to the example.com domain:

```
cluster1::> vserver cifs domain preferred-dc remove -vserver vs1 -domain  
example.com -preferred-dc 192.168.0.101
```

## vserver cifs domain preferred-dc show

Display a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver cifs domain preferred-dc show` command displays lists of preferred domain controllers by Vserver and domain.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

This parameter specifies the name of the Vserver for which you want to display preferred domain controllers.

**[-domain <TextNoCase>]** - Fully Qualified Domain Name

This parameter specifies the fully-qualified name of the domain of the domain controllers to display.

**[-preferred-dc <InetAddress>, ...]** - Preferred Domain Controllers

This parameter specifies a comma-delimited list of IP addresses for domain controllers to display.

## Examples

The following example displays all preferred domain controllers for all Vservers:

```
cluster1::> vserver cifs domain preferred-dc show
Vserver      Domain Name      Preferred Domain Controllers
-----
vs1          example.com      192.168.0.100, 192.168.0.101
```

---

## vserver cifs group-policy modify

Change group policy configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy modify` command modifies a CIFS server's group policy configuration.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver whose group policy configuration you want to modify.

**[-status {enabled|disabled}]** - Group Policy Status

This parameter specifies whether the CIFS-enabled Vserver's group policy is enabled or disabled.

### Examples

The following example enables the group policy for CIFS-enabled Vserver vs1.

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled
```

## vserver cifs group-policy show-applied

Show currently applied group policy setting

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy show-applied` command displays information about group policies assigned to a Vserver. It displays all or a subset of the group policy information matching the criteria that you specify.

---

If you do not specify any parameters, the command displays the following information about all group policies applied to Vservers in the cluster:

- GPO Name: Specifies the name of the Group Policy object.
- Level: Specifies the level in which the Group Policy is configured. It could be either site level, domain level or OU level.
- Enabled: Specifies whether this Group Policy object is enabled or not.

#### Registry Settings:

- Refresh Time Interval: Specifies how often the Group Policy is updated.
- Refresh Random Offset: Specifies a random time that is added to the refresh interval to prevent all clients from requesting Group Policy updates at the same time.
- Hash Publication for BranchCache: Specifies the hash generation mode used to generate hashes for data stored in shared folders, which is then provided to clients on which BranchCache is enabled. Possible values are:
  - per-share - Allow hash publication only for shared folders on which BranchCache is enabled.
  - disabled - Disallow hash publication on all shared folders.
  - all-shares - Allow hash publication for all shared folders.
- Hash Version Support for BranchCache: Specifies the version supported by the BranchCache hash generation service. Possible values are:
  - all-versions - Both versions 1 and 2 (V1 and V2).
  - version1 - Version 1 (V1).
  - version2 - Version 2 (V2).

#### Security Settings:

- Kerberos:
  - Max Clock Skew: Specifies maximum tolerance in hours for computer clock synchronization.
  - Max Ticket Age: Specifies maximum lifetime in minutes for user ticket.



- 
- **Max Renew Age:** Specifies maximum lifetime in days for user ticket renewal.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `-fields ?` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays only group policy information that has been applied to the Vserver you specify.

## Examples

The following example displays all group policy information about all group policies that have been applied to a Vserver:

```
cluster1::> vsriver cifs group-policy show-applied
Vserver: vs1
-----
  GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
  Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
  Security Settings:
    Kerberos:
      Max Clock Skew: 5
      Max Ticket Age: 10
      Max Renew Age: 7

  GPO Name: Resultant Set of Policy
  Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
  Security Settings:
    Kerberos:
      Max Clock Skew: 5
      Max Ticket Age: 10
      Max Renew Age: 7
2 entries were displayed.
```

---

## vserver cifs group-policy show-defined

Show applicable group policy settings defined in Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy show-defined` command displays information about group policies that have been defined in Active Directory. It displays all or a subset of the group policy configuration matching the criteria that you specify.

If you do not specify any parameters, the command displays the following information about all group policies defined in Active Directory:

- GPO Name: Specifies the name of the Group Policy object.
- Level: Specifies the level in which the Group Policy is configured. It could be either site level, domain level or OU level.
- Enabled: Specifies whether this Group Policy object is enabled or not.

Registry Settings:

- Refresh Time Interval: Specifies how often the Group Policy is updated.
- Refresh Random Offset: Specifies a random time that is added to the refresh interval to prevent all clients from requesting Group Policy updates at the same time.
- Hash Publication for BranchCache: Specifies the hash generation mode used to generate hashes for data stored in shared folders, which is then provided to clients on which BranchCache is enabled. Possible values are:
  - per-share - Allow hash publication only for shared folders on which BranchCache is enabled.
  - disabled - Disallow hash publication on all shared folders.
  - all-shares - Allow hash publication for all shared folders.
- Hash Version Support for BranchCache: Specifies the version supported by the BranchCache hash generation service. Possible values are:
  - all-versions - Both versions 1 and 2 (V1 and V2).

- 
- version1 - Version 1 (V1).
  - version2 - Version 2 (V2).

#### Security Settings:

- Kerberos:
  - Max Clock Skew: Specifies maximum tolerance in hours for computer clock synchronization.
  - Max Ticket Age: Specifies maximum lifetime in minutes for user ticket.
  - Max Renew Age: Specifies maximum lifetime in days for user ticket renewal.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays only group policy information that has been defined in Active Directory for the Vserver that you specify.

## Examples

The following example displays all group policy information for all group policies that have been defined in Active Directory:

```
cluster1:> vsriver cifs group-policy show-defined
Vserver: vs1
-----
GPO Name: Default Domain Policy
Level: Domain
Status: enabled
Registry Settings:
Refresh Time Interval: 22
Refresh Random Offset: 8
Hash Publication for BranchCache: per-share
Hash Version Support for BranchCache : version1
Security Settings:
Kerberos:
Max Clock Skew: 5
```

---

---

```
      Max Ticket Age: 10
      Max Renew Age:  7

GPO Name: Resultant Set of Policy
Status: disabled
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication for BranchCache: per-share
  Hash Version Support for BranchCache: version1
Security Settings:
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age:  7
```

---

## vserver cifs group-policy show

Show group policy configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy show` command displays information about group policy configuration for CIFS-enabled Vserver. It displays all or a subset of the group policy configuration matching the criteria that you specify.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays group policy configuration only for the Vserver that you specify.

[-status {enabled|disabled}] - Group Policy Status

If you specify this parameter, the command displays group policy configuration only for the Vservers that match the status you specify.

### Examples

The following example displays group policy configuration for all Vservers:

```
cluster1::> vserver cifs group-policy show
Vserver          GPO Status
-----
vs1              disabled
```

---

## vserver cifs group-policy update

Apply group policy settings defined in Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy update` command applies a group policy defined in Active Directory to a Vserver.

### Parameters

**-vserver** <vserver name> - Vserver Name

This parameter specifies the CIFS-enabled Vserver to which to apply the group policy.

### Examples

The following example applies a group-policy defined in Active Directory to Vserver vs1.

```
cluster1::> vserver cifs group-policy update -vserver vs1
```

## vserver cifs home-directory search-path add

Add a home directory search path

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs home-directory search-path add` command adds a search path to a CIFS home directory configuration.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver containing the CIFS home directory configuration to which you want to add the search path.

**-path** <text> - Path

---

This parameter specifies the search path you want to add.

## Examples

The following example adds the path /home1 to the CIFS home directory configuration on Vserver vs1.

```
cluster1::> vserver cifs home-directory search-path add -vserver vs1 -path /home1
```

## vserver cifs home-directory search-path remove

Remove a home directory search path

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs home-directory search-path remove` command removes a search path from a CIFS home directory configuration.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver containing the CIFS home directory configuration from which you want to remove the search path.

**-path** <text> - Path

This parameter specifies the search path you want to remove.

## Examples

The following example removes the path /home1 from the CIFS home directory configuration on Vserver vs1.

```
cluster1::> vserver cifs home-directory search-path remove -vserver vs1 -path /home1
```

## vserver cifs home-directory search-path reorder

Change the search path order used to find a match

---

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs home-directory search-path reorder` command moves a search path to a new position in the search path order in the CIFS home directory configuration for the CIFS-enabled Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS enabled Vserver for which you want to reorder searches.

**-path** <text> - Path

This parameter specifies the search path you want to move.

**-to-position** <integer> - Target Position

This parameter specifies the new position of the search path in the search path order.

## Examples

The following example moves the search path `/home1` to position 1 in the search path order for the CIFS home directory configuration on Vserver `vs1`.

```
cluster1::> vserver cifs home-directory search-path reorder -vserver vs1 -path /  
home1 -to-position 1
```

## vserver cifs home-directory search-path show

Display home directory search paths

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs home-directory search-path show` command displays information about the search paths that are in the home directory configuration for the CIFS-enabled Vservers.

## Parameters



---

{ [-fields <fieldname>, ...]

If you specify this parameter, the command only displays the fields that you specify.

| [-instance ] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays home directory configuration for the CIFS-enabled Vserver that you specify.

[-path <text>] - Path

If you specify this parameter, the command displays information only for the search path that you specify.

## Examples

The following example displays information about search paths for all CIFS home directories on all CIFS-enabled Vservers:

```
cluster1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
vs2          2      /home2
```

## vserver cifs options modify

Modify CIFS options

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs options modify` command modifies CIFS options for a CIFS server.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the CIFS server for which you want to modify CIFS options.

---

**[-default-unix-user <text>]** - Default UNIX User

This optional parameter specifies the name of the default UNIX user for the CIFS server.

**[-read-grants-exec {enabled|disabled}]** - Read Grants Exec for Mode Bits

This optional parameter specifies whether the CIFS server does read grant execution for mode bits.

**[-wins-servers <InetAddress>, ...]** - Windows Internet Name Service (WINS) Addresses

This optional parameter specifies a list of Windows Internet Name Server (WINS) addresses for the CIFS server. You must specify the WINS servers using an IP address. You can enter multiple WINS addresses as a comma-delimited list.

Note:

Use an IPv4 address because WINS over IPv6 is not supported.

**[-smb2-enabled {true|false}]** - Enable/Disable all SMB2 Protocols (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB2 version of the CIFS protocol. The default value for this parameter is true. This parameter is not supported for Vservers with Infinite Volume.

**[-smb3-enabled {true|false}]** - Enable/Disable the SMB3 Protocol (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB3 version of the CIFS protocol. The default value for this parameter is true. This parameter is not supported for Vservers with Infinite Volume.

**[-max-mpx <integer>]** - Maximum Simultaneous Operations per TCP Connection (privilege: advanced)

This optional parameter specifies the maximum number of simultaneous operations the CIFS server reports it can process per TCP connection.

**[-shadowcopy-dir-depth <integer>]** - Maximum Depth of Directories to Shadow Copy (privilege: advanced)

This optional parameter specifies the maximum depth of directories on which to create shadow copies in the CIFS server. The default for this parameter is 5. The value 0 indicates that all sub-directories should be shadow copied. This parameter is not supported for Vservers with Infinite Volume.

**[-copy-offload-enabled {true|false}]** - Enable/Disable the Copy Offload Feature (privilege: advanced)

---

This optional parameter enables the Copy Offload feature in the CIFS server. If set to false, the Copy Offload feature is disabled. The default for this parameter is true. This parameter is not supported for Vservers with Infinite Volume.

**[-default-unix-group <text>]** - Default UNIX Group

This optional parameter specifies the name of the default UNIX group for the CIFS server. If you do not specify a default UNIX group, the CIFS ACL to NFSv4 ACL translation may result in incomplete NFSv4 ACL information. This parameter is not supported by Vservers with FlexVol volumes.

**[-shadowcopy-enabled {true|false}]** - Enable/Disable the Shadow Copy Feature (VSS) (privilege: advanced)

When set to true, this optional parameter enables the Shadow Copy (VSS) feature in the CIFS server. If set to false, the Shadow Copy (VSS) feature is disabled. The default for this parameter is true. This parameter is not supported for Vservers with Infinite Volume.

**[-is-referral-enabled {true|false}]** - Refer Clients to More Optimal LIFs (privilege: advanced)

This optional parameter specifies whether the CIFS server automatically refers clients to a data LIF local to the node which hosts the root of the requested share. The default value for this parameter is false. This parameter is not supported for Vservers with Infinite Volume.

**[-is-local-auth-enabled {true|false}]** - Enable/Disable Local User Authentication (privilege: advanced)

This optional parameter specifies whether local user authentication is enabled for the CIFS server.

**[-is-local-users-and-groups-enabled {true|false}]** - Enable/Disable Local Users and Groups (privilege: advanced)

This optional parameter specifies whether the local users and groups feature is enabled for the CIFS server.

**[-is-use-junctions-as-reparse-points-enabled {true|false}]** - Enable/Disable Reparse Point Support (privilege: advanced)

This optional parameter specifies whether the CIFS server exposes junction points to Windows clients as reparse points. The default value for this parameter is true. This parameter is only active if the client has negotiated use of the SMB2 or SMB3 protocol. This parameter is not supported for Vservers with Infinite Volume.

**[-is-exportpolicy-enabled {true|false}]** - Enable/Disable Export Policies for CIFS (privilege: advanced)

---

This optional parameter specifies whether the CIFS server uses export policies to control client access. The default value for this parameter is false.

## Examples

The following example modifies CIFS options for the Vserver "vs1". It changes the default-unix-user, disables read-grants-exec, disables SMB2, changes max-mpx to 1124, and changes wins-servers to 192.168.11.112.

```
cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user pcuser  
-read-grants-exec disabled -smb2-enabled false -max-mpx 1124  
-wins-servers 192.168.11.112
```

---

## vserver cifs options show

Display CIFS options

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs options show` command displays the CIFS configuration options for one or more Vservers.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

If you specify this parameter, the command only displays CIFS options for the specified Vserver.

[-**default-unix-user** <text>] - Default UNIX User

If you specify this parameter, the command only displays CIFS options for the specified default UNIX user.

[-**read-grants-exec** {enabled|disabled}] - Read Grants Exec for Mode Bits

If you specify this parameter, the command displays CIFS options only for CIFS servers that do or do not grant execution access when granting read access using mode bits.

[-**wins-servers** <InetAddress>, ...] - Windows Internet Name Service (WINS) Addresses

If you specify this parameter, the command displays CIFS options only for CIFS servers that use the specified Windows Internet Name Server (WINS) addresses.

[-**smb2-enabled** {true|false}] - Enable/Disable all SMB2 Protocols (privilege: advanced)

---

If you specify this parameter, the command displays options only for CIFS servers that are configured to or not to negotiate the SMB2 version of the CIFS protocol.

**[-smb3-enabled {true|false}]** - Enable/Disable the SMB3 Protocol (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured to or not to negotiate the SMB3 version of the CIFS protocol.

**[-max-mpx <integer>]** - Maximum Simultaneous Operations per TCP Connection (privilege: advanced)

If you specify this parameter, the command displays the maximum number of simultaneous operations the CIFS server reports it can process per TCP connection.

**[-shadowcopy-dir-depth <integer>]** - Maximum Depth of Directories to Shadow Copy (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified depth of directories on which to create shadow copies.

**[-copy-offload-enabled {true|false}]** - Enable/Disable the Copy Offload Feature (privilege: advanced)

If set to true, this command displays options only for CIFS servers where the Copy Offload feature is enabled. If set to false, options are displayed for CIFS servers where the Copy Offload feature is disabled.

**[-default-unix-group <text>]** - Default UNIX Group

If you specify this parameter, the command displays CIFS options only for the specified default UNIX group.

**[-shadowcopy-enabled {true|false}]** - Enable/Disable the Shadow Copy Feature (VSS) (privilege: advanced)

If set to true, this command displays options only for CIFS servers where the Shadow Copy (VSS) feature is enabled. If set to false, options are displayed for CIFS servers where the Shadow Copy (VSS) feature is disabled.

**[-is-referral-enabled {true|false}]** - Refer Clients to More Optimal LIFs (privilege: advanced)

If you specify this parameter, the command displays whether the CIFS server automatically refers clients to a data LIF local to the node which hosts the root of the requested share.

**[-is-local-auth-enabled {true|false}]** - Enable/Disable Local User Authentication (privilege: advanced)

---

If this parameter is set to true, the command displays CIFS options only for CIFS servers where local user authentication is enabled. If set to false, the command displays options for CIFS servers where local user authentication is disabled.

**[-is-local-users-and-groups-enabled {true|false}]** - Enable/Disable Local Users and Groups (privilege: advanced)

If this parameter is set to true, the command displays CIFS options only for CIFS servers where the local users and groups feature is enabled. If set to false, the command displays options for CIFS servers where the local users and groups feature is disabled.

**[-is-use-junctions-as-reparse-points-enabled {true|false}]** - Enable/Disable Reparse Point Support (privilege: advanced)

If you specify this parameter, the command only displays CIFS options for Vservers which have the specified reparse point setting.

**[-is-exportpolicy-enabled {true|false}]** - Enable/Disable Export Policies for CIFS (privilege: advanced)

If you specify this parameter, the command only displays CIFS options for Vservers which have the specified export policy setting.

## Examples

The following example lists CIFS options for all Vservers on the cluster.

```
cluster1::*> vserver cifs options show
Vserver: vs1
      Copy Offload Enabled: true
      Default Unix Group: -
      Default Unix User: pcuser
      Export Policies Enabled: false
      Is Referral Enabled: false
      Is Local Auth Enabled: true
      Is Local Users and Groups Enabled: true
      Max Multiplex Count: 255
      Read Grants Exec: disabled
      Shadowcopy Dir Depth: 5
      Shadowcopy Enabled: true
      SMB2 Enabled: true
      SMB3 Enabled: true
      WINS Servers: -
      Is Use Junction as Reparse Point Enabled: true
```

---

## vserver cifs security modify

Modify CIFS security settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs security modify` command modifies CIFS server security settings.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver whose CIFS security settings you want to modify.

**[-kerberos-clock-skew <integer>]** - Maximum Allowed Kerberos Clock Skew

This parameter specifies the maximum allowed Kerberos ticket clock skew in minutes. The default is 5 minutes.

**[-kerberos-ticket-age <integer>]** - Kerberos Ticket Lifetime

This parameter specifies the Kerberos ticket lifetime in hours. The default is 10 hours.

**[-kerberos-renew-age <integer>]** - Maximum Kerberos Ticket Renewal Days

This parameter specifies the maximum Kerberos ticket renewal lifetime in days. The default is 7 days.

**[-is-signing-required {true|false}]** - Require Signing for Incoming CIFS Traffic

This parameter specifies whether signing is required for incoming CIFS traffic. The default is false.

**[-is-password-complexity-required {true|false}]** - Require Password Complexity for Local User Accounts

This parameter specifies whether password complexity is required for CIFS local users. If this parameter is set to true, password complexity is required. If the value is set to false, password complexity is not required. The default is true.

### Examples



---

The following example makes the following changes: the Kerberos clock skew is set to 3 minutes, the Kerberos ticket lifetime to 8 hours and it makes signing required for Vserver "vs1".

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew 3 -
kerberos-ticket-age 8 -is-signing-required true
```

```
cluster1::> vserver cifs security show
Vserver: vs1
Kerberos Clock Skew:          3 minutes
Kerberos Ticket Age:         8 hours
Kerberos Renewal Age:        7 days
Is Signing Required:         true
Is Password Complexity Required: true
```

## See Also

`vserver cifs security show` `vserver cifs users-and-groups local-user create`  
`vserver cifs users-and-groups local-user set-password`

---

## vserver cifs security show

Display CIFS security settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs security show` command displays information about CIFS server security settings.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

This parameter specifies the name of the Vserver whose CIFS security settings you want to display.

[-kerberos-clock-skew <integer>] - Maximum Allowed Kerberos Clock Skew

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos ticket clock skew.

[-kerberos-ticket-age <integer>] - Kerberos Ticket Lifetime

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos ticket age.

[-kerberos-renew-age <integer>] - Maximum Kerberos Ticket Renewal Days

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos renewal age.

[-realm <text>] - Kerberos Realm

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos realm.

---

**[-kdc-ip <text>, ...]** - KDC IP Address

If this parameter is specified, the command displays information only about the security settings that match the specified KDC IP address.

**[-kdc-name <text>, ...]** - KDC Name

If this parameter is specified, the command displays information only about the security settings that match the specified KDC name.

**[-site <text>, ...]** - KDC Site

If this parameter is specified, the command displays information only about the security settings that match the specified Windows site.

**[-is-signing-required {true|false}]** - Require Signing for Incoming CIFS Traffic

This parameter specifies whether signing is required for incoming CIFS traffic. If this parameter is specified, the command displays information only about the security settings that match the specified value for is-signing-required.

**[-is-password-complexity-required {true|false}]** - Require Password Complexity for Local User Accounts

If this parameter is set to true, the command displays CIFS security configuration information only for CIFS servers where password complexity for local user accounts is required. If set to false, the command displays security configuration information for CIFS servers where password complexity for local user accounts is not required.

## Examples

The following example displays CIFS server security settings.

```
cluster1::> vsriver cifs security show
Vserver: vs1
Kerberos Clock Skew:          5 minutes
Kerberos Ticket Age:         10 hours
Kerberos Renewal Age:        7 days
Is Signing Required:         false
Password Complexity Required: true
```

The following example displays the Kerberos clock skew for all Vservers.

```
cluster1::> vsriver cifs security show -fields kerberos-clock-skew
vsriver kerberos-clock-skew
-----
vs1      5
```

## See Also

`vsriver cifs security modify`

---

## vserver cifs session show

Display established CIFS sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs session show` command displays information about established CIFS sessions. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS sessions:

- Node name
- Vserver name
- CIFS connection ID
- CIFS session ID
- Workstation IP address
- CIFS user name
- CIFS open files
- Session idle time

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS sessions established on connection ID 2012, run the command with the `-connection-id` parameter set to 2012.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify this parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify this parameter, the command displays detailed information about matching CIFS sessions.

**[-node** {<nodename>|local}] - Node

---

If you specify this parameter, the command displays information about the CIFS sessions on the specified node.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information about CIFS sessions on the specified CIFS-enabled Vserver.

**[-session-id <integer>]** - Session ID

If you specify this parameter, the command displays information about the CIFS session that match the specified session ID.

**[-connection-id <integer>]** - Connection ID

If you specify this parameter, the command displays information about CIFS sessions that match the specified connection ID.

**[-lif-address <IP Address>]** - Incoming Data LIF IP Address

If you specify this parameter, the command displays information about CIFS sessions that are established through the specified data LIF IP address.

**[-address <IP Address>]** - Workstation IP address

If you specify this parameter, the command displays information about CIFS sessions that are opened from the specified IP address.

**[-auth-mechanism <Authentication Mechanism>]** - Authentication Mechanism

If you specify this parameter, the command displays information about CIFS sessions that used the specified authentication mechanism. The authentication mechanism can include one of the following:

- NTLMv1 - NTLMv1 authentication mechanism
- NTLMv2 - NTLMv2 authentication mechanism
- Kerberos - Kerberos authentication mechanism
- Anonymous - Anonymous authentication mechanism

**[-windows-user <TextNoCase>]** - Windows User

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified CIFS user. The acceptable format for CIFS user is [domain]\user.

**[-unix-user <text>]** - UNIX User

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified UNIX user.

---

**[-shares <integer>]** - Open Shares

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of CIFS shares opened.

**[-files <integer>]** - Open Files

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of regular CIFS files opened.

**[-other <integer>]** - Open Other

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of special CIFS files opened such as streams or directories.

**[-connected-time <elapsed>]** - Connected Time

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified time duration.

**[-idle-time <elapsed>]** - Idle Time

If you specify this parameter, the command displays information about CIFS sessions on which there is no activity for the specified time duration.

**[-protocol-version <CIFS Dialects>]** - Protocol Version

If you specify this parameter, the command displays information about CIFS sessions that are established over the specified version of CIFS protocol. The protocol version can include one of the following:

- SMB1 - SMB 1.0
- SMB2 - SMB 2.0
- SMB2\_1 - SMB 2.1
- SMB3 - SMB 3.0

**[-continuously-available <CIFS Open File Protection>]** - Continuously Available

If you specify this parameter, the command displays information about CIFS sessions with open files that have the specified level of continuously available protection. The open files are "continuously available" if they are opened from an SMB 3 client through a share with the "continuously\_available" property set. These open files are capable of non-disruptively recovering from takeover and giveback as well as general aggregate relocation between partners in a high-availability relationship. This is in addition to the traditional SMB 2 capability allowing clients to recover from LIF migration and other brief network interruptions.

---

## Note:

The CA protection levels depict the continuous availability at the connection level so it might not be accurate for a session if the connection has multiple sessions. Streams opened through a continuously available share are permitted, but are not currently made continuously available. Directories may be opened through a continuously available share, but, by design, will not appear continuously available as clients do not open them that way. These protection levels are applicable to the sessions on read/write volumes residing on storage failover aggregates.

The continuously available status can be one of the following:

- No - The session contains one or more open file but none of them are continuously available.
- Yes - The session contains one or more open files and all of them are continuously available.
- Partial - The session contains at least one continuously available open file but other open files that are not.

## Examples

The following example displays information about all CIFS sessions:

```
cluster1::> vservers cifs session show
Node: node1
Vserver: vs1
Connection Session
ID ID Workstation Windows User Open Files Idle Time
-----
127834 1 172.17.193.172 CIFSQA\ Administrator 2 22s
```

The following example displays information about a CIFS session with session-id 1.

```
cluster1::> vservers cifs session show -session-id 1 -instance
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.53.13.224
Workstation: 172.17.193.172
Authentication Mechanism: NTLMv2
Windows User: CIFSQA\Administrator
UNIX User: root
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 2d 17h 58m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
```

---

## vserver cifs session file show

Display opened CIFS files

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs file show` command displays information about all open CIFS files. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all open CIFS files:

- Node name
- Vserver name
- CIFS connection ID
- CIFS session ID
- CIFS file ID
- CIFS file type
- CIFS file open mode
- CIFS file hosting volume
- CIFS share name
- CIFS file path
- Continuously available protection level

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS files opened on connection ID 2012, run the command with the `-connection-id` parameter set to 2012.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify this parameter, the command only displays the fields that you specify.

| **[-instance ]** }



---

If you specify this parameter, the command displays detailed information about matching open CIFS files.

**[-node {<nodename>|local}]** - Node

If you specify this parameter, the command displays information about the open CIFS files on the specified node.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information about open CIFS files on the specified CIFS-enabled Vserver.

**[-file-id <integer>]** - File ID

If you specify this parameter, the command displays information about the open CIFS file that match the specified file ID.

**[-connection-id <integer>]** - Connection ID

If you specify this parameter, the command displays information about open CIFS files that are opened on the specified connection ID.

**[-session-id <integer>]** - Session ID

If you specify this parameter, the command displays information about the CIFS file that are opened on the specified session ID.

**[-file-type <CIFS File Type>]** - File Type

If you specify this parameter, the command displays information about opened CIFS files that are of the specified file type. The file type can be any of these: Regular, Symlink, Stream, or Directory.

**[-open-mode <CIFS Open Mode>]** - Open Mode

If you specify this parameter, the command displays information about CIFS files that are opened with the specified mode. The open mode can include one or more of the following:

- R - This property specifies that the file is opened for read.
- W - This property specifies that the file is opened for write.
- D - This property specifies that the file is opened for delete.

The open mode can have multiple values specified as a list with no commas.

**[-hosting-aggregate <aggregate name>]** - Aggregate Hosting File

If you specify this parameter, the command displays information about open CIFS files that reside on the specified aggregate.

---

**[-hosting-volume <volume name>]** - Volume Hosting File

If you specify this parameter, the command displays information about open CIFS files that reside on the specified volume.

**[-share <Share>]** - CIFS Share

If you specify this parameter, the command displays information about CIFS files that are opened over the specified CIFS share.

**[-path <text>]** - Path from CIFS Share

If you specify this parameter, the command displays information about open CIFS files that match the specified CIFS file path.

**[-share-mode <CIFS Open Mode>]** - Share Mode

If you specify this parameter, the command displays information about open CIFS files that are opened with the specified share mode. The share mode can include one or more of the following:

- R - This property specifies that the file is shared for read.
- W - This property specifies that the file is shared for write.
- D - This property specifies that the file is shared for delete.

The share mode can have multiple values specified as a list with no commas.

**[-range-locks <integer>]** - Range Locks

If you specify this parameter, the command displays information about open CIFS files that have the specified number of range locks.

**[-continuously-available <CIFS Open File Protection>]** - Continuously Available

If you specify this parameter, the command displays information about open CIFS files with or without continuously available protection. The open files are "continuously available" if they are opened from an SMB 3 client through a share with the "continuously\_available" property set. These open files are capable of non-disruptively recovering from takeover and giveback as well as general aggregate relocation between partners in a high-availability relationship. Streams opened through a continuously available share are permitted, but are not currently made continuously available. Directories may be opened through a continuously available share, but, by design, will not appear continuously available as clients do not open them that way. These protection levels are applicable to the files on read/write volumes residing on storage failover aggregates.

The continuously available status can be one of the following:

- No - The open file is not continuously available.
- Yes - The open file is continuously available.

### **[-reconnected <text>] - Reconnected**

If you specify this parameter, the command displays information about open CIFS files that have the specified reconnected state. The reconnected state can be one of the following:

- No - The open file is not reconnected.
- Yes - The open file is reconnected.

## **Examples**

The following example displays information about all open CIFS files:

```
cluster1::> vserver cifs session file show

Node:      node1
Vserver:   vs1
Connection: 2192
Session:   1
File ID    File Type    Open Mode  Hosting Volume    Share    Continuously
-----
7          Regular    rw        rootvs1          rootca    Yes
Path: \win8b8.txt
```

The following example displays information about a CIFS file with file-id 5.

```
cluster1::> vserver cifs session file show -file-id 7 -instance

Node: node1
Vserver: vs1
File ID: 7
Connection ID: 2192
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: rootvs1
CIFS Share: rootca
Path from CIFS Share: \win8b8.txt
Share Mode: rd
Range Locks: 0
Continuously Available: Yes
Reconnected: No
```

## **See Also**

vserver cifs file show

---

## vserver cifs share create

Create a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share create` command creates a CIFS share.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver on which you want to create a CIFS share.

**-share-name** <Share> - Share

This parameter specifies the name of the CIFS share that you want to create. A share name can be up to 256 characters long. If this is a home directory share (designated as such by specifying the `homedirectory` on the `-share-properties` parameter), you can include %w (Windows user name), %u (UNIX user name) and %d (Windows domain name) variables in any combination with this parameter to generate shares dynamically, with the resultant share names based on the authenticating user's Windows user name, UNIX user name, and/or Windows domain name.

**-path** <text> - Path

This parameter specifies the path to the CIFS share. This path must exist in a volume. A directory path name can be up to 256 characters long. If there is a space in the path name, you must enclose the entire string in quotation marks (for example, "/ new volume/mount here"). If this is a home directory share as specified by value of `home directory` on the `-share-properties` parameter, you can make the path name dynamic by specifying the %w (Windows user name), %u (UNIX user name), or %d (domain name) variables or any of their combination as a part of the value of this parameter.

**[-share-properties** <share properties>, ...] - Share Properties

This optional parameter specifies a list of properties for the share. The list can include one or more of the following:

- `homedirectory` - This property specifies that the share and path names are dynamic. Specify this value for a home directory share. In a home directory share,

---

Data ONTAP can dynamically generate the share's name and path by substituting %w, %u, and %d variables with the corresponding Windows user name, UNIX user name, and domain, respectively, specified as the value of the `-share-name` and `-path` parameters. For instance, if a dynamic share is defined with a name of %d\_%w, a user logged on as barbara from a domain named FIN sees the share as FIN\_barbara. Using the `homedirectory` value specifies that the share and path names are dynamically expanded. This property cannot be added or removed after share creation.

- `oplocks` - This property specifies that the share uses opportunistic locks, also known as client-side caching. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named /dept/finance contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- `browsable` - This property allows Windows clients to browse the share. This is the default initial property for all shares.
- `showsnapshot` - This property specifies that Snapshot copies can be viewed and traversed by clients.
- `changenotify` - This property specifies that the share supports ChangeNotify requests. For shares on a Vserver with FlexVol volumes, this is a default initial property. For shares on a Vserver with Infinite Volume, the `changenotify` property is not set by default, and setting it requires the advanced privilege level. When the `changenotify` property is set for a share on a Vserver with Infinite Volume, change notifications are not sent for changes to file attributes and timestamps.
- `attributecache` - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes.

Note:

For certain workloads, stale file attribute data could be delivered to a client.

- `continuously-available` - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for Vservers with Infinite Volume.
- `branchcache` - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you

---

specify per-share as the operating mode in the CIFS BranchCache configuration, and also specify the "oplocks" share property. This option is not supported for Vservers with Infinite Volume.

- **access-based-enumeration** - This property specifies that Access Based Enumeration is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

**[-symlink-properties {enable|hide|read\_only}, ...]** - Symlink Properties

This optional parameter specifies how the storage system presents UNIX symbolic links (symlinks) to CIFS clients. The list can include one or more of the following:

- **enable** - This property enables symlinks for read-write access.
- **hide** - This property hides symlinks.
- **read\_only** - This property enables symlinks for read-only access.

Note:

To disable symlinks use "" or "-".

**[-file-umask <Octal Permission>]** - File Mode Creation Mask

This optional parameter specifies the default UNIX umask for new files created on the share.

**[-dir-umask <Octal Permission>]** - Directory Mode Creation Mask

This optional parameter specifies the default UNIX umask for new directories created on the share.

**[-comment <text>]** - Share Comment

This optional parameter specifies a text comment for the share that is made available to Windows clients. The comment can be up to 256 characters long. If there is a space in the descriptive remark or the path, you must enclose the entire string in quotation marks (for example, "This is engineering's share.").

**[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]>]** - File Attribute Cache Lifetime

This optional parameter specifies the lifetime for the attribute cache share property, which you specify as the value of the -share-properties parameter.

Note:

---

This value is useful only if you specify `attributecache` as a share property.

### **[-offline-files {none|manual|documents|programs}] - Offline Files**

This optional parameter allows Windows clients to cache data on this share. The actual caching behavior depends upon the Windows client. The value can be one of the following:

- `none` - Disallows Windows clients from caching any files on this share.
- `manual` - Allows users on Windows clients to manually select files to be cached.
- `documents` - Allows Windows clients to cache user documents that are used by the user for offline access.
- `programs` - Allows Windows clients to cache programs that are used by the user for offline access and may use those files in an offline mode even if the share is available.

## **Examples**

The following example creates a CIFS share named `SALES_SHARE` on a Vserver named `vs1`. The path to the share is `/sales`.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name SALES_SHARE -  
path /sales -symlink-properties enable
```

The following example creates a CIFS share named `SALES_SHARE` on a Vserver named `vs1`. The path to the share is `/sales` and the share uses opportunistic locks (client-side caching), the share can be browsed by Windows clients, and a notification is generated when a change occurs.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name SALE -share-  
properties browsable,changenotify,oplocks
```

The following example creates a CIFS share named `DOCUMENTS` on a Vserver named `vs1`. The path to the share is `/documents` and the share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to ask for BranchCache hashes for files in the share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name DOCUMENTS path /  
documents -share-properties branchcache,changenotify,oplocks
```

The following example creates a CIFS share named `DOCUMENTS` on a Vserver named `vs1`. The path to the share is `/documents` and the share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to cache (client-side caching) user documents on this share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name DOCUMENTS -path /  
documents -share-properties changenotify,oplocks -offline-files documents
```

---

## vserver cifs share delete

Delete a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share delete` command deletes a CIFS share.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to delete a CIFS share.

**-share-name** <Share> - Share

This parameter specifies the name of the CIFS share you want to delete.

### Examples

The following example deletes a CIFS share named `share1` from a Vserver named `vs1`.

```
cluster1::> vserver cifs share delete -vserver vs1 -share-name share1
```

## vserver cifs share modify

Modify a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share modify` command modifies a CIFS share.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the CIFS-enabled Vserver containing the CIFS share you want to modify.



---

**-share-name <Share> - Share**

This parameter specifies the name of the CIFS share that you want to create. A share name can be up to 256 characters long. If this is a home directory share (designated as such by specifying the homedirectory on the `-share-properties` parameter), you can include %w (Windows user name), %u (UNIX user name) and %d (Windows domain name) variables in any combination with this parameter to generate shares dynamically, with the resultant share names based on the authenticating user's Windows user name, UNIX user name, and/or Windows domain name.

**[-path <text>] - Path**

This parameter specifies the path to the CIFS share. This path must exist in a volume. A directory path name can be up to 256 characters long. If there is a space in the path name, you must enclose the entire string in quotation marks (for example, "/new volume/mount here"). If this is a homedirectory share as specified by value of home directory on the `-share-properties` parameter, a dynamic path name must be specified using %w (Windows user name), %u (UNIX user name), or %d (domain name) variables or any of their combination as a part of the value of this parameter.

**[-symlink-properties {enable|hide|read\_only}, ...] - Symlink Properties**

This optional parameter specifies how the storage system presents UNIX symbolic links (symlinks) to CIFS clients. The list can include one or more of the following:

- enable - This property enables symlinks for read-write access.
- hide - This property hides symlinks.
- read\_only - This property enables symlinks for read-only access.

Note:

To disable symlinks use "" or "-".

**[-file-umask <Octal Permission>] - File Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new files created on the share.

**[-dir-umask <Octal Permission>] - Directory Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new directories created on the share.

**[-comment <text>] - Share Comment**

This optional parameter specifies a text comment for the share that is made available to Windows clients. The comment can be up to 256 characters long. If there is a space in

---

the descriptive remark or the path, you must enclose the entire string in quotation marks (for example, "This is engineering's share.").

**[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]>]** - File Attribute Cache Lifetime

This optional parameter specifies the lifetime for the attribute cache share property, which you specify as the value of the -share-properties parameter.

Note:

This value is useful only if you specify attributecache as a share property.

**[-offline-files {none|manual|documents|programs}]** - Offline Files

This optional parameter allows Windows clients to cache data on this share. The actual caching behavior depends upon the Windows client. The value can be one of the following:

- none - Disallows Windows clients from caching any files on this share.
- manual - Allows users on Windows clients to manually select files to be cached.
- documents - Allows Windows clients to cache user documents that are used by the user for offline access.
- programs - Allows Windows clients to cache programs that are used by the user for offline access and may use those files in an offline mode even if the share is available.

## Examples

The following example modifies a CIFS share named SALES\_SHARE on a Vserver named vs1. The share uses opportunistic locks. The file mask is set to 644 and the directory mask to 777.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name SALES_SHARE -  
symlink-properties hide -file-umask 644 -dir-umask 777
```

The following example modifies a CIFS share named SALES\_SHARE on a Vserver named vs1. The path to the share is /sales and the share uses opportunistic locks (client-side caching), the share can be browsed by Windows clients, and a notification is not generated when a change occurs.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name SALES_SHARE -  
path /sales -share-properties oplocks,browsable
```

The following example modifies a CIFS share named DOCUMENTS on a Vserver named vs1. The share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to ask for BranchCache hashes for files in the share.

---

```
cluster1::> vservers cifs share modify -vservers vs1 -share-name DOCUMENTS -share-properties branchcache,change_notify,oplocks
```

The following example modifies a CIFS share named DOCUMENTS on a Vserver named vs1. The share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to cache (client-side caching) user documents on this share.

```
cluster1::> vservers cifs share modify -vservers vs1 -share-name DOCUMENTS -share-properties change_notify,oplocks -offline-files documents
```

## Restrictions/Limitations

A CIFS client that connects to a share whose symlink properties setting is "enable" might fail to re-connect after the setting changes to "hide" under the following circumstances:

- 1) A CIFS share on the storage system has symlink properties enabled and
- 2) a client successfully connects to the share and
- 3) you disable symlink properties on the share by setting it to "hide" and
- 4) the client disconnects from the share and
- 5) the client tries to reconnect to the same share.

## vserver cifs share show

Display CIFS shares

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share show` command displays information about CIFS shares. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS shares:

- Vserver name
- CIFS share name
- Path
- Share properties
- Comment

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS shares that use

---

dynamic shares, run the command with the `-share-properties dynamicshare` parameter.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify this parameter, the command only displays the fields that you specify.

| **[-shadowcopy ]**

If you specify this parameter, the command displays information only about CIFS shadow copy shares.

| **[-umask ]**

If you specify this parameter, the command displays file and directory masks for CIFS shares.

| **[-instance ] }**

If you specify this parameter, the command displays detailed information about all CIFS shares.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information only about CIFS shares on the specified CIFS-enabled Vserver.

**[-share-name <Share>]** - Share

If you specify this parameter, the command displays information only about the CIFS share or shares that match the specified name.

**[-cifs-server <NetBIOS>]** - CIFS Server NetBIOS Name

If you specify this parameter, the command displays information only about the CIFS share or shares that use the CIFS-enabled Vserver with the specified CIFS server name.

**[-path <text>]** - Path

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified path.

**[-share-properties <share properties>, ...]** - Share Properties

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified share properties.

**[-symlink-properties {enable|hide|read\_only}, ...]** - Symlink Properties

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified symbolic link properties.

**[-file-umask <Octal Permission>]** - File Mode Creation Mask

If you specify this parameter, the command displays information only about the CIFS share or shares that use the specified file mask.

**[-dir-umask <Octal Permission>]** - Directory Mode Creation Mask

If you specify this parameter, the command displays information only about the CIFS share or shares that use the specified directory mask.

**[-comment <text>]** - Share Comment

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified comment.

**[-acl <text>, ...]** - Share ACL

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified ACL.

**[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]>]** - File Attribute Cache Lifetime

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified attribute-cache-ttl for attribute cache.

**[-volume <volume name>]** - Volume Name

If you specify this parameter, the command displays information only about the CIFS shares that are present in this volume.

**[-offline-files {none|manual|documents|programs}]** - Offline Files

If you specify this parameter, the command displays information only about the CIFS shares that have the specified Offline Files properties.

## Examples

The following example displays information about all CIFS shares:

cluster1::> vserver cifs share show			Properties	Comment	ACL
Vserver	Share	Path			
vs1	ROOTSHARE	/	oplocks browsable changenoti fy	Share mapped to top of Vserver global namespac e	CNC \ Everyone / Full Control
vs1	admin\$	/	browsable	-	-
vs1	ipc\$	/	browsable	-	-

---

3 entries were displayed.

The following example displays information about a CIFS share named SALES\_SHARE on a Vserver named vs1.

```
cluster1:> vserver cifs share show -vserver vs1 -share-name SALES_SHARE
      Vserver: vs1
      Share: SALES_SHARE
CIFS Server NetBIOS Name: WINDATA
      Path: /sales
      Share Properties: oplocks
                      browsable
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
      Offline Files: manual
```

---

## vserver cifs share access-control create

Create an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share access-control create` command adds a user or group to a CIFS share's ACL.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver containing the CIFS share.

**-share** <Share> - Share Name

This parameter specifies the name of the CIFS share.

**-user-or-group** <TextNoCase> - User/Group Name

This parameter specifies the user or group to add to the CIFS share's access control list. If you specify the user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

**-permission** <access rights> - Access Type

This parameter specifies the permissions for the user or group. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

### Examples

The following example adds the group "Everyone" with "Full\_Control" permission to the access control list of the share "vol3".

```
vs1::*> vserver cifs share access-control create -share vol3 -user-or-group Everyone -permission Full_Control
```

---

## vserver cifs share access-control delete

Delete an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share access-control delete` command deletes a user or group from a CIFS share's ACL.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver containing the CIFS share.

**-share** <Share> - Share Name

This parameter specifies the name of the CIFS share.

**-user-or-group** <TextNoCase> - User/Group Name

This parameter specifies the user or group to delete from the CIFS share's access control list. If you specify a user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

### Examples

The following example deletes the group "Everyone" for the access control list of share "vol3".

```
vs1::*> vserver cifs share access-control delete -share vol3 -user-or-group Everyone
```

## vserver cifs share access-control modify

Modify an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description



---

The `vserver cifs share access-control modify` command modifies the permissions of a user or group in a CIFS share's ACL.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver containing the CIFS share whose ACL you want to modify.

**-share** <Share> - Share Name

This parameter specifies the name of the CIFS share whose ACL you want to modify.

**-user-or-group** <TextNoCase> - User/Group Name

This parameter specifies the user or group to modify. If you specify the user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

**[-permission** <access rights>] - Access Type

This parameter specifies the permissions for the user or group. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

## Examples

The following example modifies the access control list for a share named "vol3". It changes the permission for the group "Everyone" to "Full\_Control".

```
vs1::*> vserver cifs share access-control modify -share vol3 -user-or-group Everyone -permission Full_Control
```

## vserver cifs share access-control show

Display access control lists on CIFS shares

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver cifs share access-control show` command displays the ACLs of CIFS shares.

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

This optional parameter specifies the name of the Vserver containing the share for which you want to display the access control list.

[-**share** <Share>] - Share Name

This optional parameter specifies the name of the CIFS share for which you want to display the access control list.

[-**user-or-group** <TextNoCase>] - User/Group Name

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified user or group.

[-**permission** <access rights>] - Access Type

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified permission. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

[-**winsid** <windows sid>] - Windows SID

---

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified Windows SID.

**Examples**

The following example displays all the ACLs for shares in Vserver vs1.

```
vs1::*> vsriver cifs share access-control show
Vserver      Share      User/Group      Access
              Name      Name      Permission
-----
vs1          vol3      CIFSQA\administrator      Read
vs1          vol3      Everyone      Full_Control
```

---

## vserver cifs share properties add

Add to the list of share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share properties add` command adds share properties to the list of share properties of an existing CIFS share. You can add one or more share properties. You can add additional share properties at any time by rerunning this command. Any share properties that you have previously specified will remain in effect and newly added properties are appended to the existing list of share properties.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver containing the CIFS share whose share properties you want to add.

**-share-name** <Share> - Share

This parameter specifies the name of the CIFS share.

**-share-properties** <share properties>, ... - Share Properties

This parameter specifies the list of share properties you want to add to the CIFS share. The share properties can be one or more of the following:

- **oplocks** - This property specifies that the share uses opportunistic locks, also known as client-side caching. This is a default initial property for all shares; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named `/dept/finance` contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- **browsable** - This property allows Windows clients to browse the share. This is a default initial property for all shares.

- 
- **showsnapshot** - This property specifies that Snapshot copies can be viewed and traversed by clients.
  - **changenotify** - This property specifies that the share supports Change Notify requests. For shares on a Vserver with FlexVol volumes, this is a default initial property. For shares on a Vserver with Infinite Volume, the **changenotify** property is not set by default, and setting it requires the advanced privilege level. When the **changenotify** property is set for a share on a Vserver with Infinite Volume, change notifications are not sent for changes to file attributes and timestamps.
  - **attributecache** - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes.

Note:

For certain workloads, stale file attribute data could be delivered to a client.

- **continuously-available** - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for Vservers with Infinite Volume.
- **branchcache** - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "oplocks" share property. This option is not supported for Vservers with Infinite Volume.
- **access-based-enumeration** - This property specifies that Access Based Enumeration (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

Note:

The **oplock**, **browsable**, and **changenotify** share properties are assigned to a share by default. If you have removed them from a share, you can use the **vserver cifs share properties add** command to add these properties to the share.

## Examples

The following example adds the "showsnapshot" and "changenotify" properties to a share named "sh1".

---

```
cluster::>vserver cifs share properties add -vserver vs1 -share-name sh1  
-share-properties showsnapshot,changenotify
```

## vserver cifs share properties remove

Remove from the list of share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share properties remove` command removes share properties from the list of share properties of an existing CIFS share. You can remove one or more share properties. You can remove additional share properties at any time by rerunning this command. Any existing share properties that you do not remove remain in effect.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver containing the CIFS share whose share properties you want to remove.

**-share-name** <Share> - Share

This parameter specifies the name of the CIFS share.

**-share-properties** <share properties>, ... - Share Properties

This parameter specifies the list of share properties you want to remove from the CIFS share. The share properties can be one or more of the following:

- **oplocks** - This property specifies that the share uses opportunistic locks, also known as client-side caching. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named `/dept/finance` contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- **browsable** - This property allows Windows clients to browse the share.

- 
- **showsnapshot** - This property specifies that Snapshot copies can be viewed and traversed by clients.
  - **changenotify** - This property specifies that the share supports Change Notify requests. For shares on a Vserver with FlexVol volumes, this is a default initial property. For shares on a Vserver with Infinite Volume, the **changenotify** property is not set by default, and setting it requires the advanced privilege level. When the **changenotify** property is set for a share on a Vserver with Infinite Volume, change notifications are not sent for changes to file attributes and timestamps.
  - **attributecache** - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes.

Note:

For certain workloads, stale file attribute data could be delivered to a client.

- **continuously-available** - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for Vservers with Infinite Volume.
- **branchcache** - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "oplocks" share property. This option is not supported for Vservers with Infinite Volume.
- **access-based-enumeration** - This property specifies that Access Based Enumeration (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

## Examples

The following example removes "showsnapshot" and "changenotify" properties to a share named "sh1".

```
cluster::>vserver cifs share properties remove -vserver vs1 -share-name  
sh1 -share-properties showsnapshot,changenotify
```

## vserver cifs share properties show

---

Display share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs share properties show` command displays the CIFS share properties.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

This optional parameter specifies the name of the Vserver containing the CIFS share for which you want to display share properties.

[-share-name <Share>] - Share

If you specify this parameter, the command displays share properties only for the CIFS share that you specify.

[-share-properties <share properties>, ...] - Share Properties

If you specify this parameter, the command displays share properties only for CIFS shares using the properties you specify. The share properties can be one or more of the following:

- **homedirectory** - This property specifies that the share and path names are dynamic. Specify this value for a home directory share. In a home directory share, the share's name and path can be generated by substituting `%w` and `%d` variables with the corresponding user's name and domain, respectively, specified as the value of the `-share-name` and `-path` parameters. For instance, if a dynamic share is defined with a name of `%d_%w`, a user logged on as `barbara` from a domain named `FIN` sees the share as `FIN_barbara`. Using the `homedirectory` value specifies that the share and path names are dynamically expanded.



- **oplocks** - This property specifies that the share uses opportunistic locks, also known as client-side caching.
- **browsable** - This property allows Windows clients to browse the share.
- **showsnapshot** - This property specifies that Snapshot copies can be viewed and traversed by clients.
- **changenotify** - This property specifies that the share supports Change Notify requests.
- **attributecache** - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes.

Note:

For certain workloads, stale file attribute data could be delivered to a client.

- **continuously-available** - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
- **branchcache** - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "oplocks" share property.
- **shadowcopy** - This property specifies that the share is pointing to a shadow copy. This attribute cannot be added nor removed from a share.
- **access-based-enumeration** - This property specifies that Access Based Enumeration is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

### Examples

The following example displays share properties for shares in Vserver vs1.

```
cluster::> vservers cifs share properties show
Vserver      Share      Properties
-----
vs1          abc        oplocks
              browsable
              changenotify
vs1          admin$    browsable
vs1          ipc$      browsable
vs1          shl       oplocks
              browsable
              changenotify

4 entries were displayed.
```

---

## vserver cifs superuser create

Adds superuser permissions to a CIFS account

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs superuser create` command elevates the privileges of the specified domain account in this Vserver to superuser. With superuser privileges, Data ONTAP bypasses some of the security checks.

### Parameters

**-vserver** <vserver name> - Vserver

Vserver name.

**-domain** <CIFS domain> - Domain

The domain name of accountname.

**-accountname** <CIFS account> - User

The domain account to which you want to give superuser privileges.

### Examples

The following example shows how to elevate ExampleUser in EXAMPLE domain to superuser for a Vserver vs1.

```
vs1::> vserver cifs superuser create -domain EXAMPLE -accountname ExampleUser -  
vserver vs1
```

## vserver cifs superuser delete

Deletes superuser permissions from a CIFS account

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

---

The `vserver cifs superuser delete` command removes the superuser privileges for the specified domain account in this Vserver. With superuser privileges, Data ONTAP bypasses some of the security checks.

## Parameters

**-vserver** <vserver name> - Vserver

Vserver name.

**-domain** <CIFS domain> - Domain

The domain name of accountname.

**-accountname** <CIFS account> - User

The domain account name you want to remove superuser privileges.

## Examples

The following example shows how to remove superuser privileges for ExampleUser in EXAMPLE domain for a Vserver vs1.

```
vs1::> vserver cifs superuser delete -domain EXAMPLE -accountname ExampleUser -vserver vs1
```

## vserver cifs superuser show

Display superuser permissions for CIFS accounts

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs superuser show` command displays all account names with superuser privileges. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following superuser information for all CIFS servers:

- Vserver name
- CIFS server NetBIOS name
- Domain
- Account Name

---

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays superuser information of only the specified Vservers.

[-domain <CIFS domain>] - Domain

If you specify this parameter, the command displays superuser information of only for accounts that are in the specified domain.

[-accountname <CIFS account>] - User

If you specify this parameter, the command displays superuser information of only the CIFS servers with the specified superuser account.

[-cifs-server <NetBIOS>] - CIFS Server NetBIOS Name

If you specify this parameter, the command displays superuser information of only the Vservers with specified CIFS server name.

## Examples

The following example displays superuser information of all Vservers.

```
vs1::> vserver cifs superuser show
```

Vserver	CIFS Server	Domain	Account Name
vs1	SMB_SERVER1	CIFSDOMAIN	ADMINISTRATOR
vs2	SMB_SERVER2	CIFSDOMAIN	ADMINISTRATOR

---

## vserver cifs symlink create

Create a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs symlink create` command creates a symbolic link mapping for CIFS. A mapping consists of a Vserver name, a UNIX (NFS) path, a CIFS share name, and a CIFS path. You can also specify a CIFS server name and whether the CIFS symbolic link is a local link or wide link. A local symbolic link maps to the local CIFS share, while a wide symbolic link maps to any CIFS share on the network. If the target share is a Home Directory, then the `-home-directory` field must be set to true for correct processing.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to create the mapping.

**-unix-path** <text> - UNIX Path

This parameter specifies the UNIX (NFS) path for the mapping.

Note:

It must begin and end with a forward slash (/).

**-share-name** <Share> - CIFS Share

This parameter specifies the CIFS share for the mapping.

**-cifs-path** <TextNoCase> - CIFS Path

This parameter specifies the CIFS path for the mapping. Note that this value is specified by using a UNIX-style path.

Note:

It must begin and end with a forward slash (/).

**[-cifs-server <TextNoCase>]** - Remote NetBIOS Server Name

---

This parameter specifies a new CIFS server DNS name, IP address, or NetBIOS name for the mapping.

**[-locality {local|widelink}]** - Local or Wide Symlink

This parameter specifies whether the CIFS symbolic link is a local link or wide link. A local symbolic link maps to the local CIFS share, while a wide symbolic link maps to any CIFS share on the network. The default setting is `local`.

**[-home-directory {true|false}]** - Home Directory

This parameter specifies whether the target share is a home directory. The default value is `false`.

Note:

This field must be set to `true` when the target share is a Home Directory for correct processing.

## Examples

The following example creates a symbolic link mapping on a Vserver named `vs1`. It has the UNIX path `/sales/`, the CIFS share name `SALES_SHARE`, and the CIFS path `/mycompany/sales/`.

```
cluster1::> vserver cifs symlink create -vserver vs1
-unix-path /sales/ -share-name SALES_SHARE -cifs-path "/mycompany/sales/"
```

The following example creates a symbolic link mapping on a Vserver named `vs1`. It has the UNIX path `/example/`, the CIFS share name `EXAMPLE_SHARE`, the CIFS path `/mycompany/example/`, the CIFS server IP address, and is a `widelink`.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /example/ -share-
name EXAMPLE_SHARE
-cifs-path "/mycompany/example/" -cifs-server CIFS_SERVER1 -locality widelink
```

---

## vserver cifs symlink delete

Delete a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs symlink delete` command deletes a symbolic link mapping for CIFS.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver on which the symbolic link mapping is located.

**-unix-path** <text> - UNIX Path

This specifies the UNIX (NFS) path of the mapping that you want to delete.

### Examples

The following example deletes a symbolic link mapping to a UNIX path `/example/` from a Vserver named `vs1`:

```
cluster1::> vserver cifs symlink delete -vserver vs1 -unix-path /example/
```

## vserver cifs symlink modify

Modify a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs symlink modify` command modifies the CIFS share name, CIFS path, CIFS server name, or locality of a symbolic link mapping. It can also be used to modify the value of `-home-directory` field.

### Parameters

---

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the symbolic link mapping is located.

**-unix-path** <text> - UNIX Path

This parameter specifies the UNIX (NFS) path of the mapping that you want to modify.

Note:

It must begin and end with a forward slash (/).

**[-share-name** <Share>] - CIFS Share

This parameter specifies a new CIFS share name for the mapping.

**[-cifs-path** <TextNoCase>] - CIFS Path

This parameter specifies a new CIFS path for the mapping. Note that this value is specified by using a UNIX-style path.

Note:

It must begin and end with a forward slash (/).

**[-cifs-server** <TextNoCase>] - Remote NetBIOS Server Name

This parameter specifies a new CIFS server DNS name, IP address, or NetBIOS name for the mapping.

**[-locality** {local|widelink}] - Local or Wide Symlink

This parameter specifies a new locality for the mapping. A local symbolic link maps to the local CIFS share, while a wide symbolic link maps to any CIFS share on the network. The default setting is `local`.

**[-home-directory** {true|false}] - Home Directory

This parameter specifies whether the new target share is a home directory.

Note:

This field must be set to true when the target share is a Home Directory for correct processing.

## Examples



---

The following example modifies the symbolic link mapping to a UNIX path `/example/` on a Vserver named `vs1`. The mapping is modified to use the CIFS path `/mycompany/example/`.

```
cluster1::> vserver cifs symlink modify -vserver vs1 -unix-path /example/ -cifs-path "/mycompany/example/"
```

The following example modifies the symbolic link mapping to a UNIX path `/example/` on a Vserver named `vs1`. The mapping is modified to use the CIFS share name `EXAMPLE_SHARE`, the CIFS path `/mycompany/example/`, on the CIFS server `cifs.example.com`, and to be a widelink.

```
cluster1::> vserver cifs symlink modify -vserver vs1 -unix-path /example/ -share-name EXAMPLE_SHARE -cifs-path "/mycompany/example/" -cifs-server cifs.example.com -locality widelink
```

---

## vserver cifs symlink show

Show symlink path mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs symlink show` command displays the following information about symbolic link mappings for CIFS:

- Vserver
- UNIX (NFS) path
- The DNS name, IP address, or NetBIOS name of the CIFS server
- CIFS share name
- CIFS path
- Whether the locality of the CIFS server is a local or widelink (A local symbolic link maps to the local CIFS share, while a wide symbolic link maps to any CIFS share on the network.)

### Parameters

{ [-fields <fieldname>, ...]

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

| [-instance ] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information about symbolic link mappings on the specified Vserver.

[-unix-path <text>] - UNIX Path

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified UNIX (NFS) path.

---

**[-share-name <Share>]** - CIFS Share

If you specify this parameter, the command displays information only about the symbolic link mapping or mappings that use the specified CIFS share.

**[-cifs-path <TextNoCase>]** - CIFS Path

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified CIFS path.

**[-cifs-server <TextNoCase>]** - Remote NetBIOS Server Name

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified CIFS server.

**[-locality {local|widelink}]** - Local or Wide Symlink

If you specify this parameter, the command displays information only about the symbolic link mappings that have the specified locality.

**[-home-directory {true|false}]** - Home Directory

If you specify this parameter, the command displays information only about the symbolic link mappings that have the target share as a home directory (if true) or as a static CIFS share (if false).

## Examples

The following example displays information about all symbolic link mappings for CIFS:

```
cluster1::> vsver cifs symlink show
Vserver      Unix Path  CIFS Server  CIFS Share  CIFS Path  Locality
-----
vs1          /hr/      192.0.2.160  HR_SHARE    /mycompany/hr/  widelink
vs1          /sales/   WINDATA     SALES_SHARE /mycompany/sales/ local
vs1          /web/     cifs.example.com WEB_SHARE   /mycompany/web/  widelink
3 entries were displayed.
```

The following example displays information about all symbolic link mappings that are widelinks:

```
cluster1::> vsver cifs symlink show -locality widelink
Vserver      Unix Path  CIFS Server  CIFS Share  CIFS Path  Locality
-----
vs1          /hr/      192.0.2.160  HR_SHARE    /mycompany/hr/  widelink
vs1          /web/     cifs.example.com WEB_SHARE   /mycompany/web/  widelink
2 entries were displayed.
```

---

## vserver cifs users-and-groups update-names

Update the names of Active Directory users and groups

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs users-and-groups update-names` command updates the names of Active Directory users and groups that are registered in local databases on the cluster and reports the status of the update operations. This is done so that objects that were renamed in the Active Directory can be properly displayed and configured in the local databases.

### Parameters

**-vserver** <vserver name> - Vserver

If you specify this parameter, the command will only be performed within the scope of the Vserver that matches the specified Vserver name.

{ **[-display-failed-only** {true|false}] - Display Only Failures

If you set this parameter to true, the command displays only the Active Directory users and groups that failed to update. If set to false, the command displays only the Active Directory users and groups that successfully updated.

| **[-suppress-all-output** {true|false}] } - Suppress All Output

If you set this parameter to true, the command does not display information about the status of the updates of Active Directory users and groups. To display information about the status of the updates, set this parameter to false or do not specify this parameter in the command.

### Examples

The following example updates the names of Active Directory users and groups associated with Vserver "vs1". In the last case, there is a dependent chain of names that needs to be updated.

```
cluster1::*> vserver cifs users-and-groups update-names -vserver vs1
Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated
```

---

```
Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID
"S-1-5-21-123456789-234565432-987654321-123457"
to name "dom_user5"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123458"
to name "dom_user6"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123459"
to name "dom_user7"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123460"
to name "dom_user8"
```

The command completed successfully. 7 Active Directory objects have been updated.

---

## vserver cifs users-and-groups local-group add-members

Add members to a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group add-members` command adds members to a local group.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the name of the local group.

**-member-names** <CIFS name>, ... - Names of Users or Active Directory Groups to be Added

This specifies the list of local users, Active Directory users, or Active Directory groups to be added to a particular local group.

### Examples

The following example adds a local user "CIFS\_SERVER\loc\_usr1" and an Active Directory group "CIFS\_SERVER\dom\_grp2" to the local group "CIFS\_SERVER\g1".

```
cluster1::>vserver cifs users-and-groups local-group add-members -vserver vs1 -group-name CIFS_SERVER\g1 -member-names CIFS_SERVER\loc_usr1,AD_DOMAIN\dom_grp2
```

---

## vserver cifs users-and-groups local-group create

Create a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group create` command creates a local group and optionally sets the description of that local group. The group name must meet the following criteria:

- The group name length must not exceed 256 characters.
- The group name cannot be terminated by a period.
- The group name cannot include commas.
- The group name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The group name cannot include characters in the ASCII range 1-31, which are non-printable.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the name of the local group.

**[-description** <TextNoCase>] - Description

This specifies a description for this local group. If the description contains a space, enclose the parameter in quotation marks.

### Examples

The following example creates a local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1:>vserver cifs users-and-groups local-group create -vserver vs1 -group-  
name CIFS_SERVER\g1
```

---

## vserver cifs users-and-groups local-group delete

Delete a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group delete` command deletes a local group. Removing a local group removes its membership records.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the name of the local group to delete.

### Examples

The following example deletes the local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-group delete -vserver vs1 -group-name CIFS_SERVER\g1
```

## vserver cifs users-and-groups local-group modify

Modify a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group modify` command modifies the description of a local group.

### Parameters



---

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the name of the local group.

**[-description** <TextNoCase>] - Description

This specifies a description for this local group. If the description contains a space, enclose the parameter in quotation marks.

## Examples

The following example modifies the description of the local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-group modify -vserver vs1 -group-name CIFS_SERVER\g1 -description "Example Description"
```

## vserver cifs users-and-groups local-group remove-members

Remove members from a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-group remove-members` command removes members from a local group.

## Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the name of the local group.

**-member-names** <CIFS name>, ... - Names of Users or Active Directory Groups to be Removed

---

This specifies the list of local users, Active Directory users, or Active Directory groups to be removed from a particular local group.

## Examples

The following example removes the local users "CIFS\_SERVER\u1" and "CIFS\_SERVER\u2" from the local group "CIFS\_SERVER\g1".

```
cluster1::>vserver cifs users-and-groups local-group remove-members -vserver vs1  
-group-name CIFS_SERVER\g1 -member-names CIFS_SERVER\u1,CIFS_SERVER\u2
```

---

## vserver cifs users-and-groups local-group rename

Rename a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group rename` command renames a local group. The new group name must remain in the same domain as the old group name. The new group name must meet the following criteria:

- The group name length must not exceed 256 characters.
- The group name cannot be terminated by a period.
- The group name cannot include commas.
- The group name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The group name cannot include characters in the ASCII range 1-31, which are non-printable.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-group-name** <CIFS name> - Group Name

This specifies the local group's name.

**-new-group-name** <CIFS name> - New Group Name

This specifies the local group's new name.

### Examples

The following example renames the local group "CIFS\_SERVER\g\_old" to "CIFS\_SERVER\g\_new" on Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-group rename -group-name  
CIFS_SERVER\g_old -new-group-name CIFS_SERVER\g_new -vserver vs1
```

---

## vserver cifs users-and-groups local-group show-members

Display local groups' members

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group show-members` command displays members of a local group. The members can be local or Active Directory users or groups.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays group members of local groups that match the specified Vserver name.

[-group-name <CIFS name>] - Group Name

If this parameter is specified, the command displays group members of local groups that match the specified group name.

[-member <CIFS name>] - Member Name

If this parameter is specified, the command displays group members that match the specified member name. The name can be that of a local user, Active Directory user, or Active Directory group.

### Examples

The following example displays members of local groups associated with Vserver "vs1".

---

```

cluster1::>vserver cifs users-and-groups local-group show-members -vserver vs1
Vserver      Group Name      Members
-----
vs1          BUILTIN\Administrators  CIFS_SERVER\Administrator
                                     AD_DOMAIN\Domain Admins
                                     AD_DOMAIN\dom_grpl
                                     AD_DOMAIN\Domain Users
                                     AD_DOMAIN\dom_usr1
                                     CIFS_SERVER\ul
        BUILTIN\Users
        CIFS_SERVER\gl
6 entries were displayed.

```

---

## vserver cifs users-and-groups local-group show

Display local groups

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group show` command displays local groups.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays information only about local groups that match the specified Vserver name.

[-group-name <CIFS name>] - Group Name

If this parameter is specified, the command displays information only about local groups that match the specified group name.

[-description <TextNoCase>] - Description

If this parameter is specified, the command displays information only about local groups that match the specified description.

### Examples

The following example displays all local groups associated with Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name      Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
```

---

vs1	BUILTIN\Power Users	Restricted administrative
privileges		
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\g1	
vs1	CIFS_SERVER\g2	

6 entries were displayed.

---

## vserver cifs users-and-groups local-user create

Create a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user create` command creates a local user and optionally sets the attributes for that local user. The command prompts for the local user's password.

The user name must meet the following criteria:

- The user name length must not exceed 20 characters.
- The user name cannot be terminated by a period.
- The user name cannot include commas.
- The user name cannot include any of the following printable characters: " , / \ , [ ] , : , | , < , > , + , = , ; , ? , \* , @
- The user name cannot include characters in the ASCII range 1-31, which are non-printable.

The password must meet the following criteria:

- The password must be at least six characters in length.
- The password must not contain user account name.
- The password must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~ , ! , @ , # , 0 , ^ , & , \* , \_ , - , + , = , ` , \ , | , ( , ) , [ , ] , : , ; , " , ' , < , > , , , . , ? , /

### Parameters



---

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-name** <CIFS name> - User Name

This specifies the user name.

**[-full-name** <TextNoCase>] - Full Name

This specifies the user's full name. If the full name contains a space, enclose the full name within double quotation marks.

**[-description** <TextNoCase>] - Description

This specifies a description for this local user. If the description contains a space, enclose the parameter in quotation marks.

**[-is-account-disabled** {true|false}] - Is Account Disabled

This specifies whether the user account is enabled or disabled. Set this parameter to true to disable the account. Set this parameter to false to enable the account. If this parameter is not specified, the default is to enable the user account.

## Examples

The following example creates a local user "CIFS\_SERVER\u1" associated with Vserver "vs1".

```
cluster1:>vserver cifs users-and-groups local-user create -vserver vs1 -user-name CIFS_SERVER\u1
```

```
Enter the password:  
Confirm the password:
```

## vserver cifs users-and-groups local-user delete

Delete a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-user delete` command deletes a local user. Upon deletion, all membership entries for this local user are deleted.

## Parameters

---

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-name** <CIFS name> - User Name

This specifies the user name.

## Examples

The following example deletes the local user "CIFS\_SERVER\u1" associated with Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-user show-membership
(vserver cifs users-and-groups local-user show-membership)
Vserver      User Name      Membership
-----
vs1          CIFS_SERVER\Administrator  BUILTIN\Administrators
              CIFS_SERVER\ul        CIFS_SERVER\gl
2 entries were displayed.

cluster1::>vserver cifs users-and-groups local-user delete -vserver vs1 -user-
name CIFS_SERVER\ul

cluster1::>vserver cifs users-and-groups local-user show-membership
Vserver      User Name      Membership
-----
vs1          CIFS_SERVER\Administrator  BUILTIN\Administrators
```

---

## vserver cifs users-and-groups local-user modify

Modify a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user modify` command modifies attributes of a local user.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-name** <CIFS name> - User Name

This specifies the user name.

**[-full-name** <TextNoCase>] - Full Name

This specifies the user's full name. If the full name contains a space in the name, enclose it within double quotation marks

**[-description** <TextNoCase>] - Description

This specifies a description for this local user. If the description contains a space, enclose the parameter in quotation marks.

**[-is-account-disabled** {true|false}] - Is Account Disabled

This specifies if the user account is enabled or disabled. Set this parameter to true to disable the account. Set this parameter to false to enable the account.

### Examples

The following example modifies the full name of the local user "CIFS\_SERVER\u1".

```
cluster1::>vserver cifs users-and-groups local-user modify -user-name CIFS_SERVER
\u1 -full-name "John Smith" -vserver vs1
```

## vserver cifs users-and-groups local-user rename

---

Rename a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-user rename` command renames a local user. The new user name must remain in the same domain as the old user name.

The new user name must meet the following criteria:

- The user name length must not exceed 20 characters.
- The user name cannot be terminated by a period.
- The user name cannot include commas.
- The user name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The user name cannot include characters in the ASCII range 1-31, which are non-printable.

## Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-name** <CIFS name> - User Name

This specifies the user name.

**-new-user-name** <CIFS name> - New User Name

This specifies the new user name.

## Examples

The following example renames the local user "CIFS\_SERVER\u\_old" to "CIFS\_SERVER\u\_new" on Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-user rename -user-name CIFS_SERVER
\u_old -new-user-name CIFS_SERVER\u_new -vserver vs1
```

---

## vserver cifs users-and-groups local-user set-password

Set a password for a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user set-password` command sets the password for the specified local user. The password must meet the following criteria:

- The password must be at least six characters in length.
- The password must not contain user account name.
- The password must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~, !, @, #, 0, ^, &, \*, \_, -, +, =, ` \, |, (, ), [, ], :, ;, ", ', <, >, ,, ., ?, /

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-name** <CIFS name> - User Name

This specifies the user name.

### Examples

The following example sets the password for the local user "CIFS\_SERVER\ul" associated with Vserver "vs1".

```
cluster1::>vserver cifs users-and-groups local-user set-password -user-name  
CIFS_SERVER\ul -vserver vs1
```

Enter the new password:

---

Confirm the new password:

The following example attempts to set the password but fails because the password did not meet password complexity requirements.

```
cluster1::>vserver cifs users-and-groups local-user set-password -user-name  
CIFS_SERVER\ul -vserver vs1
```

Enter the new password:

Confirm the new password:

Error: command failed: The password does not meet the password complexity requirements. Refer to the man page for details.

---

## vserver cifs users-and-groups local-user show-membership

Display local users' membership information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user show-membership` command displays the membership of local users.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

If this parameter is specified, the command displays local user membership information for local users that are associated with the specified Vserver.

[-**user-name** <CIFS name>] - User Name

If this parameter is specified, the command displays local user membership information for a local user that matches the specified user name.

[-**membership** <CIFS name>] - Local Group That This User is a Member of

If this parameter is specified, the command displays local user membership information for the local group of which this local user is a member.

### Examples

The following example displays the membership information of all local users; user "CIFS\_SERVER\Administrator" is a member of "BUILTIN\Administrators" group, and "CIFS\_SERVER\u1" is a member of "CIFS\_SERVER\g1" group.

---

```
cluster1::>vserver cifs users-and-groups local-user show-membership
Vserver      User Name      Membership
-----
vs1          CIFS_SERVER\Administrator  BUILTIN\Administrators
             CIFS_SERVER\ul         CIFS_SERVER\gl
2 entries were displayed.
```



---

## vserver cifs users-and-groups local-user show

Display local users

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user show` command displays local users and their attributes.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

If this parameter is specified, the command displays information only about local users that match the specified Vserver name.

[-**user-name** <CIFS name>] - User Name

If this parameter is specified, the command displays information only about local users that match the specified user name.

[-**full-name** <TextNoCase>] - Full Name

If this parameter is specified, the command displays information only about local users that match the specified full name.

[-**description** <TextNoCase>] - Description

If this parameter is specified, the command displays information only about local users that match the specified description.

[-**is-account-disabled** {true|false}] - Is Account Disabled

---

If this parameter is specified, the command displays information only about local users that match the status specified.

**Examples**

The following example displays information about all local users.

```
cluster1::>vserver cifs users-and-groups local-user show
Vserver      User Name      Full Name      Description
-----
vs1          CIFS_SERVER\Administrator  James Raynor    Built-in
administrator account
vs1          CIFS_SERVER\ul          Sarah Kerrigan
2 entries were displayed.
```

---

## vserver cifs users-and-groups privilege add-privilege

Add local privileges to a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege add-privilege` command adds privileges to a local or Active Directory user or group.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-or-group-name** <CIFS name> - User or Group Name

This specifies the name of the local or Active Directory user or group.

**-privileges** <Privilege>, ... - Privileges

This specifies the list of privileges to be associated with this user or group.

### Examples

The following example adds the privileges "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" to the user "CIFS\_SERVER\u1".

```
cluster1:>vserver cifs users-and-groups privilege add-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\u1 -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

---

## vserver cifs users-and-groups privilege remove-privilege

Remove privileges from a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege remove-privilege` command removes privileges from a local or Active Directory user or group. This command creates a new or modifies an existing privilege entry.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-or-group-name** <CIFS name> - User or Group Name

This specifies the name of the local or Active Directory user or group.

**-privileges** <Privilege>, ... - Privileges

This specifies the list of privileges to be removed from this user or group.

### Examples

The following example removes the previously added "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" privileges from the user "CIFS\_SERVER\u1".

```
cluster1::>vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\u1          SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::>vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\u1 -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::>vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\u1          -
```

The following example removes "SeBackupPrivilege" from the group "BUILTIN\Administrators".

```
cluster1::>vserver cifs users-and-groups privilege show
This table is currently empty.
```

---

```
cluster1::>vserver cifs users-and-groups privilege remove-privilege -vserver vs1  
-user-or-group-name BUILTIN\Administrators -privileges SeBackupPrivilege
```

```
cluster1::>vserver cifs users-and-groups privilege show
```

Vserver	User or Group Name	Privileges
vs1	BUILTIN\Administrators	SeRestorePrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege

---

## vserver cifs users-and-groups privilege reset-privilege

Reset local privileges for a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege reset-privilege` command resets privileges of a local or Active Directory user or group.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver.

**-user-or-group-name** <CIFS name> - User or Group Name

This specifies the name of the local or Active Directory user or group.

### Examples

The following example resets the privileges for the local user "CIFS\_SERVER\u1". This operation removes the privilege entry, if any, associated with the local user "CIFS\_SERVER\u1".

```
cluster1::>vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\u1          SeTakeOwnershipPrivilege
                                   SeRestorePrivilege

cluster1::>vserver cifs users-and-groups privilege reset-privilege -vserver vs1 -
user-or-group-name CIFS_SERVER\u1

cluster1::>vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group "BUILTIN\Administrators", effectively removing the privilege entry.

```
cluster1::>vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::>vserver cifs users-and-groups privilege reset-privilege -vserver vs1 -
user-or-group-name BUILTIN\Administrators

cluster1::>vserver cifs users-and-groups privilege show
```

---

This table is currently empty.

---

## vserver cifs users-and-groups privilege show

Display privileges

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege show` command displays privilege overrides assigned to local or Active Directory users or groups.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified Vserver name.

[-user-or-group-name <CIFS name>] - User or Group Name

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified user name or group name.

[-privileges <Privilege>, ...] - Privileges

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified privileges.

### Examples

The following example displays all privileges explicitly associated with local or Active Directory users or groups for Vserver "vs1".



---

```
cluster1::>vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                     SeRestorePrivilege
```

---

## vserver data-policy export

Display a data policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The vservers-data policy export command displays the current data policy for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver with Infinite Volume for which the data policy will be displayed.

### Examples

The following example shows the current data policy.

```
cluster::> vservers data-policy export -vserver vs1
{ "ruleset_format_version" : "1.0",
  "rules" : [
    { "rule_label" : "default",
      "rule_id" : "ec17a05f-7785-11e1-baf4-123478563412",
      "rule_scope" : [],
      "rule_epoch" : { "epoch_reference" : "ctime" },
      "rule_epochs" : {
        "0" : {
          "local" : {
            "metadata" : {
              "storageservice" : "-"
            }
          }
        }
      }
    }
  ]
}
```

---

## vserver data-policy import

Import a data policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The vservers data-policy import command sets a new data policy for a Vserver with Infinite Volume. After entering the command, you are prompted to type or paste the content of the new data policy. When you are done, press ENTER on a blank line.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver with Infinite Volume for which the data policy will be changed.

### Examples

The following examples attempt to change the Vserver data policy, first with bad content, and then with an acceptable data policy.

```
cluster::> vservers data-policy import -vserver vs1
Enter the contents of the file data policy for Vserver "vs1":
Press <Enter> when done
{ "foo" : "bar" }

Error: command failed: Data Policy validation failed: 'ruleset_format_version'
is a required field.

cluster::> vservers data-policy import -vserver vs1
Enter the contents of the file data policy for Vserver "vs1":
Press <Enter> when done
{ "ruleset_format_version" : "1.0",
  "rules" : {
    { "rule_label" : "default",
      "rule_id" : "ec17a05f-7785-11e1-baf4-123478563412",
      "rule_scope" : [],
      "rule_epoch" : { "epoch_reference" : "ctime" },
      "rule_epochs" : {
        "0" : {
          "local" : {
            "metadata" : {
              "storageservice" : "-"
            }
          }
        }
      }
    }
  }
}
```

---

## vserver data-policy validate

Validate a data policy without import

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The vservers data-policy validate command checks a data policy for errors, without modifying the data policy for the Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver Name

This specifies the Vserver with Infinite Volume for which the data policy will be validated.

### Examples

The following examples show first a problem with a given data policy, and then an example of a valid data policy.

```
cluster::*> vservers data-policy validate -vserver vs1
Enter the contents of the file data policy for Vserver "vs1":
Press <Enter> when done
{ "foo" : "bar" }

Error: command failed: Data Policy validation failed: 'ruleset_format_version'
is a required field.

cluster::*> vservers data-policy validate -vserver vs1
Enter the contents of the file data policy for Vserver "vs1":
Press <Enter> when done
{ "ruleset_format_version" : "1.0",
  "rules" : {
    { "rule_label" : "default",
      "rule_id" : "ec17a05f-7785-11e1-baf4-123478563412",
      "rule_scope" : [],
      "rule_epoch" : { "epoch_reference" : "ctime" },
      "rule_epochs" : {
        "0" : {
          "local" : {
            "metadata" : {
              "storageservice" : "-"
            }
          }
        }
      }
    }
  }
}
```

Data Policy validation succeeded: No errors found.

---

## vserver export-policy copy

Copy an export policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy copy` command creates a copy of an export policy on the same or a different Vserver. The command fails if an export policy with the specified new name already exists on the target Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy that you want to copy is located.

**-policyname** <text> - Policy Name

This parameter specifies the export policy that you want to copy.

**-newvserver** <vserver name> - New Vserver

This parameter specifies the Vserver to which you want to copy the export policy.

**-newpolicyname** <text> - New Export Policy Name

This parameter specifies the name of the new policy.

### Examples

The following example copies an existing policy named `read_only_expolicy` located on a Vserver named `vs0` to a new policy named `default_expolicy` located on a Vserver named `vs1`.

```
vs1::> vserver export-policy copy -vserver vs0 -policyname read_only_expolicy -  
newvserver vs1 -newpolicyname default_expolicy
```

## vserver export-policy create

Create a rule set

---

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver export-policy create` command creates an export policy. You can use the `vserver export-policy rule create` command to add rules to a policy. Each cluster has an empty default export policy with the ID 0. This default export policy does not contain any rules. You cannot delete the default export policy, but you can rename or modify it.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to create the export policy.

**-policyname** <text> - Policy Name

This parameter specifies the export policy that you want to create.

## Examples

The following example creates an export policy named `read_only_expolicy` on a Vserver named `vs0`:

```
vs1::> vserver export-policy create -vserver vs0 -policyname read_only_expolicy
```

## See Also

`vserver export-policy rule create`

---

## vserver export-policy delete

Delete a rule set

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy delete` command deletes an export policy. You cannot delete the default policy (named `default`) for a Vserver unless you delete the Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy that you want to delete is located.

**-policyname** <text> - Policy Name

This parameter specifies the export policy that you want to delete.

### Examples

The following example deletes an export policy named `test_expolicy` from a Vserver named `vs0`:

```
vs1::> vserver export-policy delete -vserver vs0 -policyname test_expolicy
```

## vserver export-policy rename

Rename an export policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rename` command renames an export policy.

### Parameters

---

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy is located.

**-policyname** <text> - Policy Name

This parameter specifies the export policy that you want to rename.

**-newpolicyname** <text> - New Export Policy Name

This parameter specifies the new name of the export policy.

## Examples

The following example renames an export policy named `user_expolicy` with the name `read_only_expolicy` on a Vserver named `vs0`:

```
vs1::> vserver export-policy rename -vserver vs0 -policyname user_expolicy -
newpolicyname read_only_expolicy
```

## vserver export-policy show

Display a list of rule sets

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver export-policy show` command displays the following information:

- Vserver name
- Export policy name
- Policy ID (diagnostic privilege level only)

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.



---

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays a list of export policies that are located on the Vserver that you specify.

**[-policyname <text>]** - Policy Name

If you specify this parameter, the command displays only the export policy or sets that match the specified name.

## Examples

The following example displays a list of all export policies:

```
vs1::> vserver export-policy show
VServer      Policy Name
-----
vs0          default_expolicy
vs0          read_only_expolicy
vs1          default_expolicy
vs1          test_expolicy
4 entries were displayed.
```

---

## vserver export-policy rule create

Create a rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rule create` command creates an export rule and adds it to a policy. To create an export rule, you must specify the following items:

- Vserver
- Export policy
- Clients that match the rule
- Read-only access rule
- Read-write access rule

You can optionally specify the following items:

- Index number; that is, the location of the export rule in the policy
- Access protocol
- Anonymous ID
- Superuser security type
- Whether `suid` access is enabled
- Whether creation of devices is enabled
- Whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited or allowed when the request originates from an NFS client (advanced privilege and higher only)
- Whether ownership changes are restricted or not (advanced privilege and higher only)

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy is located.

---

**-policyname** <text> - Policy Name

This parameter specifies the name of the export policy to which you want to add the new export rule. The export policy must already exist. To create an export policy, see the `vserver export-policy create` command.

**[-ruleindex** <integer>] - Rule Index

This optional parameter specifies the index number of the export rule that you want to create. If you specify an index number that already matches a rule, the index number of the existing rule is incremented, as are the index numbers of all subsequent rules, either to the end of the list or to an open space in the list. If you do not specify an index number, the new rule is placed at the end of the policy's list.

**[-protocol** {any|nfs3|nfs|cifs|nfs4|flexcache}, ...] - Access Protocol

This optional parameter specifies the list of access protocols for which you want to apply the export rule. Possible values include the following:

- any - Any current or future access protocol
- nfs - Any current or future version of NFS
- nfs3 - The NFSv3 protocol
- nfs4 - The NFSv4 protocol
- cifs - The CIFS protocol
- flexcache - The FlexCache protocol

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list. If you do not specify this parameter, the value defaults to any.

**-clientmatch** <text> - Client Match Hostname, IP Address, Netgroup, or Domain

This parameter specifies the client or clients to which the export rule applies. You can specify the match in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.10/4
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64

- 
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
  - As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
  - As a domain name preceded by the . character; for instance, .example.com

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

**-rorule** {any|none|never|krb5|ntlm|sys}, ... - RO Access Rule

This parameter specifies the security type for read-only access to volumes that use the export rule. Possible values include the following:

- sys - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH\_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- krb5 - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos 5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- ntlm - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- any - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) remains the same as the security type of the incoming request.

Note:

If the security type of the incoming request is AUTH\_NONE, read access will be granted to that incoming request as an anonymous user.

- none - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the rorule. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes none.

- 
- **never** - For an incoming request from a client matching the clientmatch criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as any or never, you cannot specify any other security types.

Note:

For an incoming request from a client matching the clientmatch criteria, if the security type doesn't match any of the values listed in rorule (as explained above), access will be denied to that incoming request.

**-rwrule** {any|none|never|krb5|ntlm|sys}, ... - RW Access Rule

This parameter specifies the security type for read-write access to volumes that use the export rule. Possible values include the following:

- **sys** - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH\_SYS.
- **krb5** - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos 5.
- **ntlm** - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- **any** - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

Note:

If the effective security type (determined from rorule) of the incoming request is none, write access will be granted to that incoming request as an anonymous user.

- **none** - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.

- 
- **never** - For an incoming request from a client matching the clientmatch criteria, do not allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as any or never, you cannot specify any other security types.

Note:

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

#### **[-anon <text>]** - User ID To Which Anonymous Users Are Mapped

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to when evaluation of rorule or superuser parameters result in user being mapped to the anonymous user. The default setting of this parameter is 65534, which is normally associated with the user name nobody. The following notes apply to the use of this parameter:

- To disable access by any client with a user ID of 0, specify a value of 65535.

#### **[-superuser {any|none|never|krb5|ntlm|sys}, ...]** - Superuser Security Types

This parameter specifies a security type for superuser access to files. The default setting of this parameter is none. Possible values include the following:

- **sys** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH\_SYS.
- **krb5** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos 5.
- **ntlm** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- **any** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

Note:

---

If the effective security type (determined from `rorule`) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- none - For an incoming request from a client matching the `clientmatch` criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from `rorule`) of that incoming request is none.

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as `any`, you cannot specify any other security types.

Note:

For an incoming request from a client matching the `clientmatch` criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in `superuser` (as explained above), the user ID is mapped to anonymous user.

**[-allow-suid {true|false}]** - Honor SetUID Bits in SETATTR

This parameter specifies whether set user ID (suid) and set group ID (sgid) access is enabled by the export rule. The default setting is `true`.

**[-allow-dev {true|false}]** - Allow Creation of Devices

This parameter specifies whether the creation of devices is enabled by the export rule. The default setting is `true`.

**[-ntfs-unix-security-ops {ignore|fail}]** - NTFS Unix Security Options (privilege: advanced)

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (fail) or allowed (ignore) when the request originates from an NFS client. The default setting is `fail`.

**[-chown-mode {restricted|unrestricted}]** - Change Ownership Mode (privilege: advanced)

This parameter specifies a change ownership mode. The default setting is `restricted`.

## Examples

The following example creates an export rule with index number 1 in an export policy named `read_only_expolicy` on a Vserver named `vs0`. The rule matches all clients in the domain named `example.com`. The rule enables all access protocols. It enables read-only access by any matching client and requires authentication by `AUTH_SYS`, `NTLM`, or `Kerberos 5` for read-write access. Clients with the UNIX user ID zero are mapped to

---

user ID 65534 (which normally maps to the user name nobody). It does not enable suid and sgid access or the creation of devices.

```
vs1::> vserver export-policy rule create -vserver vs0 -policyname
read_only_expolicy -ruleindex 1
-protocol any -clientmatch .example.com -rorule any -rwrule "ntlm,krb5,sys" -anon
65534 -allow-suid false
-allow-dev false
```

## See Also

vserver export-policy create



---

## vserver export-policy rule delete

Delete a rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rule delete` command deletes an export rule from a policy. You can specify the export rule by specifying its index number in the policy. When you delete a rule, the other rules in the policy are not automatically renumbered or reordered. You can use the `vserver export-policy rule setindex` command to reorder the rules in a rule set.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver which contains the export policy.

**-policyname** <text> - Policy Name

This parameter specifies the export policy from which you want to delete a rule.

**-ruleindex** <integer> - Rule Index

This parameter specifies the index number of the rule that you want to delete. You can use the `vserver export-policy rule show` command to view a list of rules with their index numbers.

### Examples

The following example deletes an export rule with the index number 5 from an export policy named `rs1` on a Vserver named `vs0`:

```
vs1::> vserver export-policy rule delete -vserver vs0  
-policyname read_only_expolicy -ruleindex 5
```

### See Also

`vserver export-policy rule show`   `vserver export-policy rule setindex`

---

## vserver export-policy rule modify

Modify a rule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rule modify` command modifies a specified export rule in a policy. This command cannot change the position of a rule in a policy; to reorder rules in a policy, use the `vserver export-policy rule setindex` command. You can use this command to change the following attributes of an export rule:

- Access protocol
- Client match specification
- Read-only access rule
- Read-write access rule
- Anonymous ID
- Superuser security type
- Whether suid access is enabled
- Whether creation of devices is enabled
- Whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited or allowed when the request originates from an NFS client (advanced privilege and higher only)
- Whether ownership changes are restricted or not (advanced privilege and higher only)

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy is located.

**-policyname** <text> - Policy Name

This parameter specifies the name of the export policy containing the export rule that you want to modify.

---

**-ruleindex** <integer> - Rule Index

This parameter specifies the index number of the export rule that you want to modify. To view a list of rules with their index numbers, use the `vserver export-policy rule show` command.

**[-protocol** {any|nfs3|nfs|cifs|nfs4|flexcache}, ...] - Access Protocol

This optional parameter specifies the list of access protocols for which you want to apply the export rule. Possible values include the following:

- any - Any current or future access protocol
- nfs - Any current or future version of NFS
- nfs3 - The NFSv3 protocol
- nfs4 - The NFSv4 protocol
- cifs - The CIFS protocol
- flexcache - The FlexCache protocol

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list. If you do not specify this parameter, the value defaults to any.

**[-clientmatch** <text>] - Client Match Hostname, IP Address, Netgroup, or Domain

This parameter specifies the client or clients to which the export rule applies. You can specify the match in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.10/4
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

---

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

**[-rorule {any|none|never|krb5|ntlm|sys}, ...]** - RO Access Rule

This parameter modifies the security type for read-only access to volumes that use the export rule. Possible values include the following:

- **sys** - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH\_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- **krb5** - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos 5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- **ntlm** - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- **any** - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) remains the same as the security type of the incoming request.

Note:

If the security type of the incoming request is AUTH\_NONE, read access will be granted to that incoming request as an anonymous user.

- **none** - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the rorule. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes none.
- **never** - For an incoming request from a client matching the clientmatch criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as any or never, you cannot specify any other security types.

---

Note:

For an incoming request from a client matching the `clientmatch` criteria, if the security type doesn't match any of the values listed in `rorule` (as explained above), access will be denied to that incoming request.

**[-rwrule {any|none|never|krb5|ntlm|sys}, ...]** - RW Access Rule

This parameter modifies the security type for read-write access to volumes that use the export rule. Possible values include the following:

- `sys` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is `AUTH_SYS`.
- `krb5` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is Kerberos 5.
- `ntlm` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is CIFS NTLM.
- `any` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume regardless of the effective security type (determined from `rorule`) of that incoming request.

Note:

If the effective security type (determined from `rorule`) of the incoming request is `none`, write access will be granted to that incoming request as an anonymous user.

- `none` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume as an anonymous user if the effective security type (determined from `rorule`) of that incoming request is `none`.
- `never` - For an incoming request from a client matching the `clientmatch` criteria, do not allow write access to the volume regardless of the effective security type (determined from `rorule`) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as `any` or `never`, you cannot specify any other security types.

Note:

---

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

**[-anon <text>]** - User ID To Which Anonymous Users Are Mapped

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to when evaluation of rorule or superuser parameters result in user being mapped to the anonymous user. The default setting of this parameter is 65534, which is normally associated with the user name nobody. The following notes apply to the use of this parameter:

- To disable access by any client with a user ID of 0, specify a value of 65535.

**[-superuser {any|none|never|krb5|ntlm|sys}, ...]** - Superuser Security Types

This parameter specifies a security type for superuser access to files. The default setting of this parameter is none. Possible values include the following:

- sys - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH\_SYS.
- krb5 - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos 5.
- ntlm - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- any - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

Note:

If the effective security type (determined from rorule) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- none - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as any, you cannot specify any other security types.

---

Note:

For an incoming request from a client matching the clientmatch criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in superuser (as explained above), the user ID is mapped to anonymous user.

**[-allow-suid {true|false}]** - Honor SetUID Bits in SETATTR

This parameter specifies whether set user ID (suid) and set group ID (sgid) access is enabled by the export rule. The default setting is `true`.

**[-allow-dev {true|false}]** - Allow Creation of Devices

This parameter specifies whether the creation of devices is enabled by the export rule. The default setting is `true`.

**[-ntfs-unix-security-ops {ignore|fail}]** - NTFS Unix Security Options (privilege: advanced)

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (fail) or allowed (ignore) when the request originates from an NFS client. The default setting is `fail`.

**[-chown-mode {restricted|unrestricted}]** - Change Ownership Mode (privilege: advanced)

This parameter specifies a change ownership mode. The default setting is `restricted`.

## Examples

The following example modifies the export rule with index number 3 in an export policy named `default_expolicy` on a Vserver named `vs0`. The rule is modified to match any clients in the netgroup named `group1` to enable NFSv2 and CIFS support, to enable read-only access by any matching client, to require authentication by NTLM or Kerberos 5 for read-write access, and to enable suid and sgid access.

```
vs1::> vserver export-policy rule modify -vserver vs0 -policyname
default_expolicy -ruleindex 3 -protocol "nfs2,cifs"
-clientmatch @group1 -rorule any -rwrule "ntlm,krb5" -allow-suid true
```

## See Also

`vserver export-policy rule show`   `vserver export-policy rule setindex`

---

## vserver export-policy rule setindex

Move a rule to a specified index

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rule setindex` command modifies the index number of the specified export rule. If the new index number is already in use, the command reorders the list to accommodate it. If the existing index is given a higher index number (that is, later in the list), the command decrements the index numbers of rules between the moved rule and moved-to rule; otherwise, the command increments the index numbers between the moved-to rule and the existing rule.

You can use the `vserver export-policy rule show` command to view a list of rules with their index numbers.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy is located.

**-policyname** <text> - Policy Name

This parameter specifies the export policy that contains the rule whose index number you want to modify.

**-ruleindex** <integer> - Rule Index

This parameter specifies the index number of the rule that you want to move.

**-newruleindex** <integer> - Index

This parameter specifies the new index number for the rule.

### Examples

The following example changes the index number of a rule at index number 5 to index number 3 in an export policy named `rs1` on a Vserver named `vs0`:

```
vs1::> vserver export-policy rule setindex -vserver vs0  
-policyname read_only_policy -ruleindex 5 -newruleindex 3
```

### See Also



---

vserver export-policy rule show

---

## vserver export-policy rule show

Display a list of rules

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver export-policy rule show` command displays information about export rules. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information:

- Vserver name
- Export policy name
- Export rule index number
- Access protocol
- Client match
- Read-only access rule
- Read-write access rule

To display detailed information about a specific export rule, run the command with the `-vserver`, `-policyname`, and `-ruleindex` parameters. The detailed view provides all of the information in the previous list and the following additional information:

- Anonymous ID
- Superuser security type
- Whether set user ID (suid) and set group ID (sgid) access is enabled
- Whether creation of devices is enabled
- NTFS security settings
- Change ownership mode

You can specify additional parameters to display only the information that matches those parameters. For example, to display information only about export rules that have a read-write rule value of `never`, run the command with the `-rwrule never` parameter.

---

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| **[-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the `-policyname` parameter, and the `-ruleindex` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules on the specified Vserver.

**[-policyname <text>]** - Policy Name

If you specify this parameter, the `-vserver` parameter, and the `-ruleindex` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules on the specified policy.

**[-ruleindex <integer>]** - Rule Index

If you specify this parameter, the `-vserver` parameter, and the `-policyname` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules that have the specified index number.

**[-protocol {any|nfs3|nfs|cifs|nfs4|flexcache}, ...]** - Access Protocol

If you specify this parameter, the command displays information only about the export rules that have the specified access protocol or protocols. Possible values include the following:

- any - Any current or future access protocol
- nfs - Any current or future version of NFS
- nfs3 - The NFSv3 protocol
- nfs4 - The NFSv4 protocol
- cifs - The CIFS protocol
- flexcache - The FlexCache protocol

---

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list.

**[-clientmatch <text>]** - Client Match Hostname, IP Address, Netgroup, or Domain

If you specify this parameter, the command displays information only about the export rules that have the specified client match. You can specify the match in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.10/4
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

**[-rorule {any|none|never|krb5|ntlm|sys}, ...]** - RO Access Rule

If you specify this parameter, the command displays information only about the export rule or rules that have the specified read-only rule. Possible values include the following:

- sys - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH\_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- krb5 - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos 5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- ntlm - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- any - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used

---

subsequently in evaluation of `rwrule/superuser`) remains the same as the security type of the incoming request.

Note:

If the security type of the incoming request is `AUTH_NONE`, read access will be granted to that incoming request as an anonymous user.

- `none` - For an incoming request from a client matching the `clientmatch` criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the `rorule`. The effective security type of the incoming request (to be used subsequently in evaluation of `rwrule/superuser`) becomes `none`.
- `never` - For an incoming request from a client matching the `clientmatch` criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as `any` or `never`, you cannot specify any other security types.

Note:

For an incoming request from a client matching the `clientmatch` criteria, if the security type doesn't match any of the values listed in `rorule` (as explained above), access will be denied to that incoming request.

**`[-rwrule {any|none|never|krb5|ntlm|sys}, ...]`** - RW Access Rule

If you specify this parameter, the command displays information only about the export rule or rules that have the specified read-write rule. Possible values include the following:

- `sys` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is `AUTH_SYS`.
- `krb5` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is Kerberos 5.
- `ntlm` - For an incoming request from a client matching the `clientmatch` criteria, allow write access to the volume if the effective security type (determined from `rorule`) of that incoming request is CIFS NTLM.

- 
- any - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

Note:

If the effective security type (determined from rorule) of the incoming request is none, write access will be granted to that incoming request as an anonymous user.

- none - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- never - For an incoming request from a client matching the clientmatch criteria, do not allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as any or never, you cannot specify any other security types.

Note:

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

**[-anon <text>]** - User ID To Which Anonymous Users Are Mapped

If you specify this parameter, the command displays information only about the export rule or rules that have the specified anonymous ID.

**[-superuser {any|none|never|krb5|ntlm|sys}, ...]** - Superuser Security Types

If you specify this parameter, the command displays information only about the export rule or rules that have the specified superuser security type. Possible values include the following:

- sys - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH\_SYS.
- krb5 - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos 5.

- 
- **ntlm** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
  - **any** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

Note:

If the effective security type (determined from rorule) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- **none** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- **never** - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user regardless of the effective security type (determined from rorule) of that incoming request.

Note:

Only export rules that were created in an earlier release can have the superuser parameter set to the security type never

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as any, you cannot specify any other security types.

Note:

For an incoming request from a client matching the clientmatch criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in superuser (as explained above), the user ID is mapped to anonymous user.

**[-allow-suid {true|false}]** - Honor SetUID Bits in SETATTR

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for set user ID (suid) and set group ID (sgid) access.

**[-allow-dev {true|false}]** - Allow Creation of Devices

---

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for the creation of devices.

**[-ntfs-unix-security-ops {ignore|fail}]** - NTFS Unix Security Options (privilege: advanced)

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for the Vserver. The setting can either prohibit (fail) or allow (ignore) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client.

**[-ntfs-unix-security-ops-vs <NfsNtfsUnixSecOps>]** - Vserver NTFS Unix Security Options (privilege: advanced)

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for the Vserver. The setting can either prohibit (fail) or allow (ignore) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client.

**[-chown-mode {restricted|unrestricted}]** - Change Ownership Mode (privilege: advanced)

If you specify this parameter, the command displays information only about the export rule or rules that have the specified change ownership mode.

**[-chown-mode-vs {restricted|unrestricted|use-export-policy}]** - Vserver Change Ownership Mode (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified change ownership mode setting.

## Examples

The following example displays information about all export rules:

```
vs1::> vsserver export-policy rule show
Vserver      Policy      Rule      Access   Client      RO
Name         Name         Index    Protocol Match      Rule
-----
vs0          default_expolicy 1        any      0.0.0.0/0  any
vs0          read_only_expolicy 2        any      0.0.0.0/0  any
vs1          default_expolicy 1        any      0.0.0.0/0  any
vs1          test_expolicy 1        any      0.0.0.0/0  any
4 entries were displayed.
```



---

## vserver fcp create

Create FCP service configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a FCP service for a Vserver. A FCP service must be licensed before you can manage FCP services. If the FCP service is not licensed, the FCP command returns an error.

When you create a FCP service on a Vserver, the Vserver has the following configuration defaults:

- The administrative status of the FCP service is up.
- The FCP command automatically generates a unique World Wide Node Name (WWNN) unless you specify one.

The format for a WWNN is XX:XX:XX:XX:XX:XX:XX:XX where X is a hexadecimal digit. When selecting a new WWNN, use the following format to fit with the registered names: 2X:XX:00:0a:98:XX:XX:XX where XX is some integral value. If your unique WWNN does not match this format, use the `-f` parameter. To modify a target-name, use the `vserver fcp modify` command.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**[-target-name** <text>] - Target Name (privilege: advanced)

Specifies the World Wide Node Name (WWNN). The format for a WWNN is XX:XX:XX:XX:XX:XX:XX:XX where X is a hexadecimal digit. To be compatible with existing registered names, the format for a new WWNN should be 2X:XX:00:0a:98:XX:XX:XX, where X is a hexadecimal digit. If the unique WWNN does not match this format, use the `-f` parameter.

**[-status-admin** {down|up}] - Administrative Status

Specifies the configured administrative status of an FCP service. If you set this parameter to up, the command displays all FCP services with the administrative status

---

of up. If you set this parameter to down, the command displays all FCP services with the administrative status of down.

**[-force | -f [true]]** - Force (privilege: advanced)

When this parameter is used, the command accepts a WWNN that is not in the valid format of 2X:XX:0a:09:80:XX:XX:XX.

## Examples

```
cluster1::> vserver fcp create -vserver vs_1
```

Creates a FCP service on Vserver vs\_1.

## See Also

vserver fcp modify

---

## vserver fcp delete

Delete FCP service configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Deletes an FCP service of a Vserver. Before you can delete an FCP service, the administration status must be "down". Use the `vserver fcp modify` command to change the administration status.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

### Examples

```
cluster1::> vserver fcp delete -vserver vs_1
```

Deletes the FCP service on Vserver vs\_1.

### See Also

`vserver fcp modify`

---

## vserver fcp modify

Modify FCP service configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command modifies an FCP service configuration on a Vserver.

If the target name provided is outside the vendor's namespace, the user must verify that the target name is unique outside the cluster. The vendor cannot verify that the target name is unique outside the cluster if the vendor did not generate the target name.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**[-target-name** <text>] - Target Name (privilege: advanced)

Specifies the World Wide Node Name (WWNN). The format for a WWNN is XX:XX:XX:XX:XX:XX:XX:XX where X is a hexadecimal digit. To be compatible with existing registered names, the format for a new WWNN should be 2X:XX:00:0a:98:XX:XX:XX, where X is a hexadecimal digit. If the unique WWNN does not match this format, use the -f parameter.

**[-status-admin** {down|up}] - Administrative Status

Specifies the configured administrative status of an FCP service. If you set this parameter to up, the command displays all FCP services with the administrative status of up. If you set this parameter to down, the command displays all FCP services with the administrative status of down.

**[-force | -f** [true]] - Force (privilege: advanced)

When this parameter is used, the command accepts a WWNN that is not in the valid format of 2X:XX:0a:09:80:XX:XX:XX.

### Examples

```
cluster1::> vserver fcp modify -vserver vs_1 -status-admin down
```

---

The example above changes the administration status of the FCP service on Vserver vs\_1 to down.

---

## vserver fcp show

Display FCP service configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Displays the current status of the FCP service in a cluster.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver Name

Use this parameter to display the FCP services that match the Vserver that you specify.

[-**target-name** <text>] - Target Name (privilege: advanced)

Use this parameter to display the FCP service that matches the target name that you specify.

[-**status-admin** {down|up}] - Administrative Status

Use this parameter to display the FCP services that match the administrative status that you specify.

### Examples

```
cluster1::> vserver fcp show
```

Vserver	Target Name	Status Admin
vs0	20:00:00:a0:98:0c:b0:eb	up
vs2	20:01:00:a0:98:0c:b0:eb	up

2 entries were displayed.

Displays the FCP configuration for all the Vservers in the cluster.

---

## vserver fcp start

Starts the FCP service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command starts the FCP service of a Vserver. When you start the FCP service, the logical interfaces are brought online.

You must have a license before you can start the FCP service. Use `system license add` to enable the FCP license.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

### Examples

```
cluster1::> vserver fcp start -vserver vs_1  
(vserver fcp start)
```

Starts a FCP service for Vserver vs\_1.

### See Also

`system license add`

---

## vserver fcp stop

Stops the FCP service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command stops the FCP service of a Vserver. When you stop the FCP service, the operation status of all FCP logical interfaces in the vserver will be "down".

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

### Examples

```
cluster1::> vserver fcp stop -vserver vs_1  
(vserver fcp stop)
```

Stops FCP service on Vserver vs\_1.



---

## vserver fcp initiator show

Display FCP initiators currently connected

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays information about FCP initiators that are currently logged in.

If you do not specify a Vserver, the command displays all initiators logged into all FCP Vservers within a cluster. If you specify a Vserver but not a logical interface, the command displays information about all initiators connected to all logical interfaces within the specified Vserver.

If an initiator belongs to an initiator group or has a World Wide Port Name (WWPN) alias, the command displays this information.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display the FCP initiators logged into the Vserver that you specify.

[-**lif** <lif-name>] - Logical Interface

Use this parameter to display the FCP initiators that match the logical interfaces that you specify.

[-**wwpn** <text>] - Initiator WWPN

Use this parameter to display the FCP initiators that matches the World Wide Port Name (WWPN) that you specify.

[-**port-address** <Hex Integer>] - Port Address

---

Use this parameter to display FCP initiators that match the port address that you specify.

**[-wwnn <text>]** - Initiator WWNN

Use this parameter to display the FCP initiator that matches the World Wide Node Name (WWNN) that you specify.

**[-alias <text>, ...]** - Initiator WWPN Alias

Use this parameter to display the FCP initiator that matches the alias name that you specify.

**[-igroup <text>, ...]** - Igroup Name

Use this parameter to display the FCP initiator that matches the initiator group that you specify.

### Examples

```
cluster1::> vserver fcp initiator show
Vserver      Logical   Initiator      Initiator
Interface    WWNN        WWPN           Igroup
-----
vs_1         vs_1.fcp    2f:a2:00:a0:98:0b:56:13
                                     2f:a2:00:a0:98:0b:56:15
                                     igroup_1
```

Displays information regarding logged in FCP initiators for Vserver vs\_1.

---

## vserver fcp interface show

Display configuration information for an FCP interface

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays FCP logical interface information. If you do not specify a Vserver, the command displays all of the FCP data interfaces of a cluster.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Use this parameter with other options to display information about FCP logical interfaces scoped to the specified Vserver.

[-lif <lif-name>] - Logical Interface

Use this parameter to display FCP logical interfaces that match the names of logical interfaces that you specify. You can provide a partial logical interface name, and press tab to complete the name or the closest match.

[-wwpn <text>] - WWPN

Use this parameter to display FCP logical interfaces that match the World Wide Port Name (WWPN) that you specify.

[-wwnn <text>] - WWNN

Use this parameter to display FCP logical interfaces that match the World Wide Node Name (WWNN) that you specify.

[-status-admin {up|down}] - Administrative Status

---

Specifies the configured status of the FCP logical interface. If you set this parameter to up the command displays all FCP logical interfaces with the administrative status of up. If you set this parameter to down the command displays all the FCP logical interfaces with the administrative status of down.

**[-status-oper {up|down}] - Operational Status**

Specifies the current status of the FCP logical interface. If you set this parameter to up the command displays all the FCP logical interfaces with the operational status of up. If you set this parameter to down the command displays all the FCP logical interfaces with the operational status of down.

**[-status-extended <text>] - Extended Status**

Use this parameter to display more detailed information on the status of the FCP logical interface that you specify.

**[-port-address <Hex Integer>] - Host Port Address**

Use this parameter to display FCP logical interfaces that match the host port address that you specify.

**[-curr-node <nodename>] - Current Node**

Use this parameter to display FCP logical interfaces that are on the node that you specify.

**[-curr-port {<netport>|<ifgrp>}] - Current Port**

Use this parameter to display FCP logical interfaces that are on the port that you specify.

**[-is-home {true|false}] - Is Home**

Specifies whether the node hosting the FCP interface is the initially configured node. If you use this command without using this parameter, it is set to true, and the command displays all FCP interfaces that are on the initially configured node.

**[-relative-port-id <integer>] - Relative Port ID**

Use this parameter to display FCP logical interfaces that matches the relative target port ID that you specify. The system assigns each LIF and target portal group a relative target port ID that is Vserver unique. You cannot change this ID.

## Examples

```
cluster1::> vserver fcp interface show
```

Vserver	Logical Interface	Status Admin/Oper	WWPN	Current Node	Current Port	Is Home
vs_a	vs_a.fcp	up/down	2f:a2:00:a0:98:0b	56:13 Node 1	0c	true

---

Displays FCP interface information on Vserver vs\_a.

---

## vserver fcp portname set

Assigns a new WWPN to a FCP adapter

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command assigns a new World Wide Port Name (WWPN) to a logical interface. To use this command, the administrative status of the logical interface must be down.

If the target name provided is outside the vendor's namespace, the user must verify that the target name is unique outside the cluster. The vendor cannot verify that the target name is unique outside the cluster if the vendor did not generate the target name.

Use the `network interface modify` to change the administration status of the logical interface.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-lif** <lif-name> - Logical Interface

Specifies the logical interface to receive a new WWPN.

**-wwpn** <text> - FCP Adapter WWPN

Specifies a new World Wide Port Name (WWPN).

To be compatible with existing registered names, the format for a new WWPN should be 2X:XX:00:0a:98:XX:XX:XX, where X is a hexadecimal digit. If the unique WWPN does not match this format, use the **-f** parameter.

**[-force | -f [true]]** - Force

When this parameter is used, the command accepts a WWPN that is not in the valid format of 2X:XX:0a:09:80:XX:XX:XX.

### Examples

```
cluster1::*> vserver fcp portname set -vserver vs_1 -lif vs_1.fcp -wwpn  
2f:a2:00:a0:98:0b:56:13
```

---

Sets a new WWPN for LIF vs\_1.fcp on Vserver vs\_1.

## **See Also**

network interface modify

---

## vserver fcp portname show

Display WWPN for FCP logical interfaces

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays a list of World Wide Port Names (WWPN) that are used by the FCP logical interfaces.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Use this parameter to display a list of FCP logical interfaces and their WWPNs that match the Vserver name you specify.

[-lif <lif-name>] - Logical Interface

Use this parameter to display a list of FCP logical interfaces and their WWPNs that match the logical interface that you specify. You can use wildcards in the logical interface to display a specific group of logical interfaces.

[-wwpn <text>] - WWPN

Use this parameter to display a list of FCP logical interfaces and their WWPNs that match the WWPN that you specify. You can use wildcards in the WWPN to display a specific group of WWPNs.

### Examples

```
cluster1::> vserver fcp portname show
Vserver      Logical      WWPN
Interface
-----
```



---

vs_a	vs_a.fcp	2f:a2:00:a0:98:0b:56:13
vs_iol	vs_iol.fcp	2f:9e:00:a0:98:0b:56:13
vs_2	lif2	2f:a3:00:a0:98:0b:56:13
vs_2	lif3	2f:a4:00:a0:98:0b:56:13
vs_2	lif4	2f:a5:00:a0:98:0b:56:13
vs_2	lif5	2f:a6:00:a0:98:0b:56:13
vs_2	vs_2.fcp	2f:9a:00:a0:98:0b:56:13
vs1	vs1.fcp	2f:9d:00:a0:98:0b:56:13
vs1	vs1.fcp2	2f:97:00:a0:98:0b:56:13

Displays the WWPNs for each FCP logical interface for all the Vservers in a cluster.

---

## vserver fcp wwpn-alias remove

Removes an alias for a World Wide Port Name of an initiator.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command removes an alias from a World Wide Port Name (WWPN).

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

{ **-alias** | **-a** <text>, ... - Initiator WWPN Alias

Specifies the alias of the WWPN that you want to remove.

| **-wwpn** | **-w** <target\_eui> } - Initiator WWPN

Specifies the WWPN.

### Examples

```
cluster1::> vserver fcp wwpn-alias remove -vserver vs_1 -wwpn  
2f:a0:00:a0:98:0b:56:13
```

On Vserver vs\_1, removes all the aliases on WWPN 2f:a0:00:a0:98:0b:56:13.

```
cluster1::> vserver fcp wwpn-alias remove -vserver vs_1 -alias my_alias
```

On Vserver vs\_1, removes the alias my\_alias.

---

## vserver fcp wwpn-alias set

Set an alias for a World Wide Port Name of an initiator that might login to the target.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates a new alias for a World Wide Port Name (WWPN). You can create multiple aliases for a WWPN, but you cannot use the same alias for multiple WWPNs.

An alias name can contain:

- Up to 32 alphanumeric characters
- Hyphen (-)
- Underscore (\_)
- Left brace ({)
- Right brace (})
- Period (.)

An alias must not contain spaces.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver.

**-alias** | **-a** <text> - Initiator WWPN Alias

Specifies the alias of the WWPN.

**-wwpn** | **-w** <target\_eui> - Initiator WWPN

Specifies the WWPN.

**[-force | -f [true]]** - Force

Allows you to override a WWPN associated with an existing alias with a newly specified WWPN. If you use this parameter without a value, it is set to true, and the command does not prompt you when you override an existing alias.

---

## Examples

```
cluster1::> vservers fcp wwpn-alias set -vservers vs_1 -alias my_alias -wwpn  
2f:a0:00:a0:98:0b:56:13
```

Sets the alias `my_alias` for the WWPN `2f:a0:00:a0:98:0b:56:13`.

---

## vserver fcp wwpn-alias show

Displays a list of the WWPN aliases configured for initiators

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays aliases associated with World Wide Port Names (WWPN).

Note:

You can also use these commands to display WWPN aliases:

- `lun igroup show`
- `lun igroup create`
- `lun igroup add`
- `lun igroup remove`
- `vserver fcp show`

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver Name

Use this parameter to display a list of WWPNs and the associated aliases that match the Vserver name that you specify.

**[-alias | -a <text>]** - Initiator WWPN Alias

Use this parameter to display the WWPN that matches the alias that you specify.

---

**[-wwpn | -w <target\_eui>]** - Initiator WWPN

Use this parameter to display a list of aliases that match the WWPN that you specify.

## Examples

```
cluster1::> vsserver fcp wwpn-alias show
Vserver      Initiator      Initiator
WWPN                                     Alias
-----
vs_1         2f:a0:00:a0:98:0b:56:13  my_alias
```

Displays the alias my\_alias for the WWPN 2f:a0:00:a0:98:0b:56:13 on Vserver vs\_1.

## See Also

lun igroup show   lun igroup create   lun igroup add   lun igroup remove  
vsserver fcp show

---

## vserver fpolicy disable

Disable a policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy disable` command disables an FPolicy policy for the specified Vserver.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to disable an FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy you want to disable.

### Examples

The following command disables an FPolicy policy.

```
Cluster::>vserver fpolicy show
Vserver      Policy Name      Sequence  Status  Engine
-----
vs1          vs1_pol          -         off     native
vs2          vs2_pol          -         on      external
2 entries were displayed.

Cluster::>vserver fpolicy disable -vserver vs2 -policy-name vs2_pol

Cluster::>vserver fpolicy show
Vserver      Policy Name      Sequence  Status  Engine
-----
vs1          vs1_pol          -         off     native
vs2          vs2_pol          5         off     external
2 entries were displayed.
```

---

## vserver fpolicy enable

Enable a policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy enable` command enables FPolicy policies for the specified Vserver and sets their sequence (priority). The sequence is used when multiple policies have subscribed to the same file access event. To modify the sequence number of a policy, the administrator must disable the policy (if it is enabled) and then use this command to enable it with the new sequence number. Policies that use the native engine configuration will have a higher priority than policies for any other engine, regardless of the sequence number assigned to them.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to enable an FPolicy policy. The Vserver administrator can enable FPolicy policies created within the scope of the Vserver and can also enable an FPolicy policy created by the cluster administrator. The cluster administrator can enable FPolicy policies for any Vserver but cannot enable them with a scope of cluster. The scope is determined at a Vserver level.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy you want to enable.

**-sequence-number** <integer> - Policy Sequence Number

This parameter specifies the sequence number which will be assigned to the policy.

### Examples

The following command enables an FPolicy policy.

```
Cluster::>vserver fpolicy show
Vserver      Policy Name      Sequence  Status Engine
-----
```



---

```
vs1          vs1_pol          -  off    native
vs2          vs2_pol          -  off    external
2 entries were displayed.
```

```
Cluster::>vserver fpolicy enable -vserver vs2 -policy-name vs2_pol -sequence-
number 5
```

```
Cluster::>vserver fpolicy show
Vserver      Policy Name      Sequence  Status  Engine
-----
vs1          vs1_pol          -         off    native
vs2          vs2_pol          5         on     external
2 entries were displayed.
```

---

## vserver fpolicy engine-connect

Establish a connection to FPolicy server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy engine-connect` command connects an FPolicy server to a specified node. Connecting the FPolicy server to a node enables FPolicy processing, providing the FPolicy configuration is complete. Before connecting an FPolicy server to a node, you must configure FPolicy by completing the following tasks:

- Create an FPolicy event
- Create an FPolicy external engine
- Create an FPolicy policy
- Create a scope for the FPolicy policy

Note:

The FPolicy event and external engine must be attached to the FPolicy policy.

Note:

The FPolicy policy should be enabled.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node that you want to connect to the FPolicy server. The value `local` specifies the current node.

**-vserver** <vserver name> - Vserver

---

This parameter specifies the Vserver that you want to connect to the specified FPolicy server using the specified FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy that is attached to an external engine.

**-server** <IP Address> - Server

This parameter specifies the FPolicy server to which you want to connect the node. The specified server must be present in the external engine configuration of the above specified policy.

### Examples

The following example connects an FPolicy server.

```
Cluster::> vservers fpolicy engine-connect -node FPolicy-01 -vservers vs1 -policy-name p -server 1.1.1.1
```

```
Cluster::> vservers fpolicy show
```

FPolicy	Vserver	Policy	Node	Server	Server-status	Server-type
	vs1	p	FPolicy-01	1.1.1.1	connected	primary

---

## vserver fpolicy engine-disconnect

Terminate connection to FPolicy server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy engine-disconnect` command disconnects an FPolicy server from a specified node.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-node** {<nodename>|local} - Node

This parameter specifies the node that you want to disconnect from the FPolicy server. The value `local` specifies the current node.

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver that you want to disconnect from the specified FPolicy server with the specified attached FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy that is attached with an external engine.

**-server** <IP Address> - Server

This parameter specifies the FPolicy server you want to disconnect. The specified server must be present in the external engine configuration of the above specified FPolicy policy.

### Examples

The following example disconnects an FPolicy server.

```
Cluster::>vserver fpolicy engine-disconnect -node FPolicy-01 -vserver vs1 -  
policy-name p -server 1.1.1.1
```

```
Cluster::>vserver fpolicy show
```

---

FPolicy Vserver	Policy	Node	Server	Server- status	Server- type
vs1	p	FPolicy-01	1.1.1.1	disconnected	primary

---

## vserver fpolicy show-enabled

Display all enabled policies

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy show-enabled` command displays information about all enabled policies in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name
- Policy name
- Priority

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies.

You can specify the `-instance` parameter to display information for all FPolicy policies in a list format.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver>]** - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver.

---

**[-policy-name <Policy name>]** - Policy Name

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

**[-priority <text>]** - Policy Priority

If you specify this parameter, the command displays information only about the FPolicy policies with the policy priority that you specify.

**Examples**

The following example displays the information about enabled FPolicy policies on the cluster.

```
Cluster::>vserver fpolicy show-enabled
Vserver          Policy Name          Priority
-----
vs1              pol_native          native
vs1              pol_native2         native
vs1              pol1                2
vs1              pol2                4
```

---

## vserver fpolicy show-engine

Display FPolicy server status

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy show-engine` command displays status information for all FPolicy external engines or displays status information only for FPolicy servers for a specified Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information for all FPolicy servers:

- Vserver name
- Node name
- FPolicy policy name
- FPolicy server IP Address
- FPolicy server status
- FPolicy server type

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy servers. You can specify specific parameters to display only information that matches those parameters. For instance, to display information only about all FPolicy servers (external engines) that are connected, run the command with the `-fields` parameter set to `server` and `-server-status` parameter set to `connected`.

You can specify the `-instance` parameter to display all information for all policies in the list form.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]



---

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-node <nodename>|local]** - Node

If you specify this parameter, the command displays information only about the FPolicy external engine attached to the specified node.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information only about the FPolicy server for the specified Vserver.

**[-policy-name <Policy name>]** - Policy

If you specify this parameter, the command displays information only about the FPolicy servers that are attached with the specified policy.

**[-server <IP Address>]** - Server

If you specify this parameter, the command displays information only about the FPolicy servers that you specify.

**[-server-status <Status>]** - Server Status

If you specify this parameter, the command displays information only about the FPolicy servers that have the specified status.

**[-server-type <Server Type>]** - Server Type

If you specify this parameter, the command displays information only about the FPolicy servers that have the specified server type.

**[-connected-since <MM/DD/YYYY HH:MM:SS>]** - Time FPolicy Server was Connected

If you specify this parameter, the command displays information only about the FPolicy servers that have been connected since the specified time.

**[-disconnected-since <MM/DD/YYYY HH:MM:SS>]** - Time FPolicy Server was Disconnected

If you specify this parameter, the command displays information only about the FPolicy servers that have been disconnected since the specified time.

**[-disconnect-reason <text>]** - Reason for FPolicy Server Disconnection

If you specify this parameter, the command displays information only about the FPolicy servers that are disconnected because of the specified reason.

**[-disconnect-reason-id <integer>]** - ID for FPolicy Server Disconnection

If you specify this parameter, the command displays information about the FPolicy servers that are disconnected because of the specified disconnect reason ID. There is a unique ID associated with each disconnect reason, which can be used to identify the reason for FPolicy server disconnection.

**[-session-id <text>]** - Session ID

If you specify this parameter, the command displays information about the FPolicy server that is connected with the specified session ID. There is a unique session ID associated with each connection to FPolicy server, which can be used to identify the established connection.

### Examples

This example displays information about all FPolicy servers (external engines).

```
Cluster::>vserver fpolicy show-engine
FPolicy
Vserver Policy Node Server Server-
-----
vs2 vs2_pol FPolicy-01 9.9.9.9 connected primary
vs1 vs1_pol FPolicy-01 1.1.1.1 connected primary
2 entries were displayed.
```

This example displays information only about all connected FPolicy servers (external engines).

```
Cluster::>vserver fpolicy show-engine -fields server -server-status connected
node vserver policy-name server
-----
FPolicy-01 vs1 vs1_pol 1.1.1.1
```

This example displays information about an FPolicy server.

```
Cluster::>vserver fpolicy show-engine -server 10.72.204.118 -instance
Node: fpol-01
Vserver: vserver_1
Policy: pol_cifs
Server: 10.72.204.118
Server Status: disconnected
Server Type: primary
Time FPolicy Server was Connected: -
Time FPolicy Server was Disconnected: 2/5/2013 05:06:22
Reason for FPolicy Server Disconnection: TCP Connection to FPolicy server failed.
ID for FPolicy Server Disconnection: 9307
Session ID:
```

---

## vserver fpolicy show

Display all policies with status

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy show` command displays status information about all FPolicy policies in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name
- Policy name
- Sequence number
- Status

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies.

You can specify the `-instance` parameter to display information for all FPolicy policies in a list format.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver** <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver.

**[-policy-name <Policy name>]** - Policy

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

**[-sequence-number <integer>]** - Sequence Number

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified sequence-number.

**[-status {on|off}]** - Status

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified status.

**[-engine <Engine name>]** - FPolicy Engine

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified engine.

### Examples

The following example displays the information about FPolicy policies on the cluster using the `vserver fpolicy show` command.

Cluster::>vserver fpolicy show			
Status	Engine	Vserver	Sequence
		Policy	Number
-----	-----	-----	-----
		FPolicy	
eng1		cserver_policy	- off
eng2	vs1	vlp1	- off
native	vs1	vlp2	- off
native	vs1	vlp3	- off
eng1	vs1	cserver_policy	- off
native	vs2	vlp1	3 on
eng3	vs2	vlp2	1 on
eng1	vs2	cserver_policy	2 on
8 entries were displayed.			

---

## vserver fpolicy policy create

Create a policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy create` command creates an FPolicy policy. You must create an FPolicy event name before creating an FPolicy policy. If you are using an external FPolicy server, you must also create an FPolicy engine before creating a policy.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy that you want to create. An FPolicy policy name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_" and ".".

**-events** <Event name>, ... - Events to Monitor

This parameter specifies a list of events to monitor for the FPolicy policy. All the events in the event list should be created by the administrator of the specified Vserver or the cluster administrator. The events must already exist. Create events using the `fpolicy policy event create` command.

**-engine** <Engine name> - FPolicy Engine

This parameter specifies an external engine for this FPolicy policy. An external engine contains information required by the node to send notifications to an FPolicy server. The Vserver administrator of the specified Vserver or the cluster administrator creates the external engine prior to creating the FPolicy policy. If this parameter is not specified,

---

the default native external engine is used. The native external engine is internal to Data ONTAP and is used if you want to configure native file blocking and you do not want to use an external FPolicy server.

**[-is-mandatory {true|false}]** - Is Mandatory Screening Required

This parameter specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances. To allow file access events under these circumstances, set this parameter to false. By default, it is true.

**[-allow-privileged-access {yes|no}]** - Allow Privileged Access

This parameter specifies privileged access for FPolicy servers. It is used to specify whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. With this option set to yes, FPolicy servers can access files on the cluster using a separate data channel with privileged access. By default, it is no.

**[-privileged-user-name <text>]** - User Name for Privileged Access

This parameter specifies the privileged user name. It is used to specify the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\user name" format. If -allow-privileged-access is set to no, any value set for this field is ignored.

## Examples

The following example creates an FPolicy policy.

```
Cluster::>vserver fpolicy policy create -vserver vs1 -policy-name vs1_pol
    -events cserver_evt,vle1 -engine native -is-mandatory true -allow-
privileged-access no
Cluster::>vserver fpolicy policy show -vserver vs1 -policy-name vs1_pol
    Vserver: vs1
    Policy Name: vs1_pol
    Events to Monitor: cserver_evt, vle1
    FPolicy Engine: native
    Is Mandatory Screening Required: true
    Allow Privileged Access: no
    User Name for Privileged Access: -
```

## See Also

fpolicy policy event create

---

## vserver fpolicy policy delete

Delete a policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy delete` command deletes an FPolicy policy.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete the FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy that you want to delete.

### Examples

The following example deletes an FPolicy policy.

```
Cluster::>vserver fpolicy policy delete -vserver vs1 -policy-name vs1_pol
```

## vserver fpolicy policy modify

Modify a policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy modify` command modifies an FPolicy policy.

---

Note:

This command is not supported for a Vserver with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy policy.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy that you want to modify. An FPolicy policy name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_" and ".".

**[-events** <Event name>, ...] - Events to Monitor

This parameter specifies a list of events to monitor for the FPolicy policy. All the events in the event list should be created by the administrator of the specified Vserver or the cluster administrator. The events must already exist. Create events using the `fpolicy policy event create` command.

**[-engine** <Engine name>] - FPolicy Engine

This parameter specifies an external engine for this FPolicy policy. An external engine contains information required by the node to send notifications to an FPolicy server. The Vserver administrator of the specified Vserver or the cluster administrator creates the external engine prior to modifying the FPolicy policy. If this parameter is not specified, the default native external engine is used. The native external engine is internal to Data ONTAP and is used if you want to configure native file blocking and you do not want to use an external FPolicy server.

**[-is-mandatory** {true|false}] - Is Mandatory Screening Required

This parameter specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances. To allow file access events under these circumstances, set this parameter to false. By default, it is true.

**[-allow-privileged-access** {yes|no}] - Allow Privileged Access

This parameter specifies privileged access for FPolicy servers. It is used to specify whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. With this option set



---

to yes, FPolicy servers can access files on the cluster using a separate data channel with privileged access. By default, it is no.

**[-privileged-user-name <text>]** - User Name for Privileged Access

This parameter specifies the privileged user name. It is used to specify the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\user name" format. If `-allow-privileged-access` is set to no, any value set for this field is ignored.

## Examples

The following example modifies an FPolicy policy.

```
Cluster::>vserver fpolicy policy modify -vserver vs1 -policy-name vs1_pol
    -events cserver_evt,vle1 -engine native -is-mandatory true -allow-
privileged-access no
Cluster::>vserver fpolicy policy show -vserver vs1 -policy-name vs1_pol
    Vserver: vs1
    Policy Name: vs1_pol
    Events to Monitor: cserver_evt, vle1
    FPolicy Engine: native
    Is Mandatory Screening Required: true
    Allow Privileged Access: no
    User Name for Privileged Access: -
```

## See Also

`fpolicy policy event create`

---

## vserver fpolicy policy show

Display policy configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy show` command displays information about all FPolicy policies belonging to the Vserver. Any Vserver administrator can see FPolicy policies associated with their Vserver as well as policies created by the cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name
- Policy name
- Events to monitor
- FPolicy engine
- Is mandatory screening required
- Allow privileged access
- User name for privileged access

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies. You can specify additional parameters to display only information that matches those parameters. For example, to display information only about FPolicy policies where the FPolicy server requires privileged access, run the command with the `-fields` parameter set to `policy-name` (no "-") and `-allow-privileged-access` parameter set to `yes`.

You can specify the `-instance` parameter to display all information for all policies in the list form.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

---

{ [-**fields** <fieldname>, ...]

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

| [-**instance** ] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-**vserver** <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver. FPolicy policies created by the cluster administrator are visible for all Vservers.

[-**policy-name** <Policy name>] - Policy

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

[-**events** <Event name>, ...] - Events to Monitor

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified event or events.

[-**engine** <Engine name>] - FPolicy Engine

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified engine.

[-**is-mandatory** {true|false}] - Is Mandatory Screening Required

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified mandatory attribute.

[-**allow-privileged-access** {yes|no}] - Allow Privileged Access

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified privileged access.

[-**privileged-user-name** <text>] - User Name for Privileged Access

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified privileged user name.

## Examples

The following example displays the information about FPolicy policies on the cluster using the `vserver fpolicy policy show` command.

---

```

Cluster::>vserver fpolicy policy show
Vserver      Policy      Events      Engine      Is Mandatory  PrivAccess
-----
Cluster      cserver_pol  cserver_   cserver_eng  true          yes
vs1          p            r          n            true          no
vs1          cserver_pol  cserver_   cserver_eng  true          yes
vs2          cserver_pol  cserver_   cserver_eng  true          yes
4 entries were displayed.

```

The following example displays FPolicy policy name information about all Vserver FPolicy policies with the `-allow-privileged-access` parameter set to "yes".

```

Cluster::> vserver fpolicy policy show -fields policy-name -allow-privileged-
access yes
vserver policy-name
-----
Cluster cserver_pol
vs1     cserver_pol
vs2     cserver_pol
3 entries were displayed.

```

---

## vserver fpolicy policy event create

Create an event

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy event create` command creates an FPolicy event. An event describes what to monitor. An event can contain protocol, file operations, filters, and volume operation event types. In the FPolicy configuration, an event is attached to an FPolicy policy. You can attach the same event to one or more policies.

Note:

This command is not supported for a Vserver with Infinite Volume.

Note:

There is dependency in three fields (`-protocol`, `-files-operations`, `-filters`) and the following are the valid combination of the three fields:

- `-protocol cifs -file-operations open,close`
- `-protocol cifs -file-operations open,close -filters monitor-ads,offline-bit`
- Specify none of the three (`-protocol`, `-files-operations`, `-filters`) fields

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy event.

**-event-name** <Event name> - Event

This parameter specifies the name of the FPolicy event that you want to create. An event name can be up to 256 characters long. An event name value is a string that can

---

only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_" and ".".

**[-protocol <Protocol>] - Protocol**

This parameter specifies the protocol name for which the event will be created. By default, no protocol is selected. The value of this parameter must be one of the following:

- cifs - This specifies that the event is for the CIFS protocol.
- nfsv3 - This specifies that the event is for the NFSv3 protocol.
- nfsv4 - This specifies that the event is for the NFSv4 protocol.

Note:

If you specify `-protocol`, then you must also specify a valid value for the `-file-operations` parameter.

**[-file-operations <File Operation>, ...] - File Operations**

This parameter specifies a list of file operations for the FPolicy event. The event will check the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. The list can include one or more of the following operations:

- close - File close operations.
- create - File create operations.
- create\_dir - Directory create operations.
- delete - File delete operations.
- delete\_dir - Directory delete operations.
- getattr - Get attribute operations.
- link - Link operations.
- lookup - Lookup operations.
- open - File open operations.
- read - File read operations.
- write - File write operations.
- rename - File rename operations.
- rename\_dir - Directory rename operations.

- 
- `setattr` - Set attribute operations.
  - `symlink` - Symbolic link operations.

Note:

If you specify `-file-operations` then you must specify a valid protocol in the `-protocol` parameter.

#### **`[-filters <Filter>, ...]` - Filters**

This parameter specifies a list of filters of given file operation or operations for the protocol specified in the `-protocol` parameter. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

- `monitor-ads` - Filter the client request for alternate data stream.
- `close-with-modification` - Filter the client request for close with modification.
- `close-without-modification` - Filter the client request for close without modification.
- `first-read` - Filter the client request for first read.
- `first-write` - Filter the client request for first write.
- `offline-bit` - Filter the client request for offline bit set. Setting this filter, FPolicy server receives notification only when offline files are accessed.
- `open-with-delete-intent` - Filter the client request for open with delete intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.
- `open-with-write-intent` - Filter the client request for open with write intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to write something in it.
- `write-with-size-change` - Filter the client request for write with size change.

Note:

If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

#### **`[-volume-operation {true|false}]` - Is Volume Operation Required**

This parameter specifies volume operation for which event will be created. By default, it is false.

---

# Examples

The following example creates an FPolicy event.

```
Cluster::> vserver fpolicy policy event create -vserver vs1 -event-
name cifs_event -protocol cifs
open,close,read,write -filters first-read,offline-bit -file-operations
true -volume-operation

Cluster::> vserver fpolicy policy event show -vserver vs1 -event-name
cifs_event
Vserver: vs1
Event Name: cifs_event
Protocol: cifs
File Operations: open, close, read, write
Filters: first-read, offline-bit
Volume Operation: true
```

The following is a list of supported `-file-operations` and `-filters` for the CIFS protocol.

Supported file operations	Supported filters
=====	
close	: monitor-ads, close-with-modification, close-without-
modification, offline-bit	
create	: monitor-ads, offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: monitor-ads, offline-bit
delete_dir	: currently no filter is supported for this file operation
getattr	: offline-bit
open	: monitor-ads, offline-bit, open-with-delete-intent, open-with-
write-intent	
read	: monitor-ads, first-read, offline-bit
write	: monitor-ads, first-write, offline-bit, write-with-size-change
rename	: offline-bit, monitor-ads
rename_dir	: currently no filter is supported for this file operation
setattr	: offline-bit, monitor-ads

The following is a list of supported `-file-operations` and `-filters` for the nfsv3 protocol.

Supported file operations	Supported filters
=====	
create	: offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: offline-bit
delete_dir	: currently no filter is supported for this file operation
link	: offline-bit
lookup	: offline-bit
read	: offline-bit
write	: offline-bit, write-with-size-change
rename	: offline-bit
rename_dir	: currently no filter is supported for this file operation
setattr	: offline-bit
symlink	: offline-bit



The following is a list of supported `-file-operations` and `-filters` for the `nfsv4` protocol.

Supported file operations	Supported filters
close	: offline-bit
create	: offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: offline-bit
delete_dir	: currently no filter is supported for this file operation
getattr	: offline-bit
link	: offline-bit
lookup	: offline-bit
open	: offline-bit
read	: offline-bit
write	: offline-bit, write-with-size-change
rename	: offline-bit
rename_dir	: currently no filter is supported for this file operation
setattr	: offline-bit
symlink	: offline-bit

---

## vserver fpolicy policy event delete

Delete an event

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy event delete` command deletes an FPolicy event.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to delete an FPolicy event.

**-event-name** <Event name> - Event

This parameter specifies the name of the FPolicy event you want to delete.

### Examples

The following example deletes an FPolicy event.

```
Cluster::>vserver fpolicy policy event delete -vserver vs1 -event-name  
cifs_event
```

## vserver fpolicy policy event modify

Modify an event

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy event modify` command modifies an FPolicy event. An event describes what to monitor. An event can contain protocol, file

---

operations, filters, and volume operation event types. In the FPolicy configuration, an event is attached to an FPolicy policy. You can attach the same event to one or more policies. You can modify an event while it is attached to an FPolicy policy. Any changes to the event take effect immediately.

Note:

This command is not supported for a Vserver with Infinite Volume.

Note:

There is dependency in three fields (`-protocol`, `-files-operations`, `-filters`) and the following are the valid combination of the three fields:

- `-protocol cifs -file-operations open,close`
- `-protocol cifs -file-operations open,close -filters monitor-ads,offline-bit`
- Specify none of the three (`-protocol`, `-files-operations`, `-filters`) fields

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy event.

**-event-name** <Event name> - Event

This parameter specifies the name of the FPolicy event that you want to modify. An event name can be up to 256 characters long. An event name value is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_" and ".".

**[-protocol** <Protocol>] - Protocol

This parameter specifies the protocol name for which the event will be modified. By default, no protocol is selected. The value of this parameter must be one of the following:

- `cifs` - This specifies that the event is for the CIFS protocol.
- `nfsv3` - This specifies that the event is for the NFSv3 protocol.
- `nfsv4` - This specifies that the event is for the NFSv4 protocol.

---

Note:

If you specify `-protocol`, then you must also specify a valid value for the `-file-operations` parameter.

**[-file-operations <File Operation>, ...] - File Operations**

This parameter specifies a list of file operations for the FPolicy event. The event will check the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. The list can include one or more of the following operations:

- close - File close operations.
- create - File create operations.
- create\_dir - Directory create operations.
- delete - File delete operations.
- delete\_dir - Directory delete operations.
- getattr - Get attribute operations.
- link - Link operations.
- lookup - Lookup operations.
- open - File open operations.
- read - File read operations.
- write - File write operations.
- rename - File rename operations.
- rename\_dir - Directory rename operations.
- setattr - Set attribute operations.
- symlink - Symbolic link operations.

Note:

If you specify `-file-operations` then you must specify a valid protocol in the `-protocol` parameter.

**[-filters <Filter>, ...] - Filters**

---

This parameter specifies a list of filters of given file operation or operations for the protocol specified in the `-protocol` parameter. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

- `monitor-ads` - Filter the client request for alternate data stream.
- `close-with-modification` - Filter the client request for close with modification.
- `close-without-modification` - Filter the client request for close without modification.
- `first-read` - Filter the client request for first read.
- `first-write` - Filter the client request for first write.
- `offline-bit` - Filter the client request for offline bit set. Setting this filter, FPolicy server receives notification only when offline files are accessed.
- `open-with-delete-intent` - Filter the client request for open with delete intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.
- `open-with-write-intent` - Filter the client request for open with write intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to write something in it.
- `write-with-size-change` - Filter the client request for write with size change.

Note:

If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

### **`[-volume-operation {true|false}]` - Is Volume Operation Required**

This parameter specifies volume operation for which event will be modified. By default, it is false.

## **Examples**

The following example modifies an FPolicy event.

```
Cluster::> vservers fpolicy policy event modify -vservers vs1 -event-  
name cifs_event -protocol cifs  
open,close,read,write -filters first-read,offline-bit -file-operations  
true -volume-operation  
Cluster::> vservers fpolicy policy event show -vservers vs1 -event-name  
cifs_event  
Vservers: vs1
```

---

```
Event Name: cifs_event
Protocol: cifs
File Operations: open, close, read, write
Filters: first-read, offline-bit
Volume Operation: true
```

The following is a list of supported `-file-operations` and `-filters` for the CIFS protocol.

Supported file operations	Supported filters
=====	
close	: monitor-ads, close-with-modification, close-without-
modification, offline-bit	
create	: monitor-ads, offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: monitor-ads, offline-bit
delete_dir	: currently no filter is supported for this file operation
getattr	: offline-bit
open	: monitor-ads, offline-bit, open-with-delete-intent, open-with-
write-intent	
read	: monitor-ads, first-read, offline-bit
write	: monitor-ads, first-write, offline-bit, write-with-size-change
rename	: offline-bit, monitor-ads
rename_dir	: currently no filter is supported for this file operation
setattr	: offline-bit, monitor-ads

The following is a list of supported `-file-operations` and `-filters` for the nfsv3 protocol.

Supported file operations	Supported filters
=====	
create	: offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: offline-bit
delete_dir	: currently no filter is supported for this file operation
link	: offline-bit
lookup	: offline-bit
read	: offline-bit
write	: offline-bit, write-with-size-change
rename	: offline-bit
rename_dir	: currently no filter is supported for this file operation
setattr	: offline-bit
symlink	: offline-bit

The following is a list of supported `-file-operations` and `-filters` for the nfsv4 protocol.

Supported file operations	Supported filters
=====	
close	: offline-bit
create	: offline-bit
create_dir	: currently no filter is supported for this file operation
delete	: offline-bit
delete_dir	: currently no filter is supported for this file operation
getattr	: offline-bit
link	: offline-bit
lookup	: offline-bit
open	: offline-bit
read	: offline-bit

---

---

write	:	offline-bit, write-with-size-change
rename	:	offline-bit
rename_dir	:	currently no filter is supported for this file operation
setattr	:	offline-bit
symlink	:	offline-bit

---

## vserver fpolicy policy event show

Display events

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy event show` command displays information about all FPolicy events belonging to the Vserver. Any Vserver administrator can see FPolicy events associated with their Vserver as well as FPolicy events created by the cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy events:

- Vserver name
- FPolicy event name
- Protocol name
- List of file operations
- List of filters
- Volume operation

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy events. You can specify additional parameters to display only information that matches those parameters. For example, to display information only about all CIFS events configured with the `-volume-operation` field set, run the command with the `-fields` parameter set to `-event-name event-name -protocol cifs -volume-operation yes`.

You can specify the `-instance` parameter to display all information for all policies in a list format.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]



If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information only about the FPolicy events for the specified Vserver. Events created on the admin Vserver by the cluster administrator are visible in all Vservers.

**[-event-name <Event name>]** - Event

If you specify this parameter, the command displays information only about the FPolicy event that matches the specified event name.

**[-protocol <Protocol>]** - Protocol

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified protocol.

**[-file-operations <File Operation>, ...]** - File Operations

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified file operation or operations.

**[-filters <Filter>, ...]** - Filters

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified filter or filters.

**[-volume-operation {true|false}]** - Is Volume Operation Required

If you set this parameter to `true`, the commands displays information about events where the `-volume-operation` parameter is set `true` . If you set this parameter to `false`, the command displays information about events where the `-volume-operation` parameter is set `false`.

## Examples

The following example displays the information about all Vserver FPolicy policy events.

```
Cluster::> vserver fpolicy policy event show
           Event                               File
Volume
Operation  Vserver  Name                      Protocols Operations  Filters
-----
true       Cluster  cserver_evt          cifs             open, close,      first-write,
                                           read, write      first-read
```

---

true	vs1	cserver_evt	cifs	open, close,	first-write,
-	vs1	vle1	cifs	read, write	first-read
false	vs1	vle2	cifs	open	-
true	vs1	vle3	nfsv4	open	-
true	vs2	cserver_evt	cifs	open, close,	first-write,
				read, write	first-read

6 entries were displayed.

The following example displays event name information about all Vserver FPolicy policy events with CIFS as a protocol and with false as volume operation.

```
Cluster::>vserver fpolicy policy event show -fields event-name -
protocol cifs -volume-operation false
vserver event-name
-----
vs1      vle2
```

## vserver fpolicy policy external-engine create

Create an external engine

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy external-engine create` command creates an FPolicy external engine. The cluster uses the external engine to hold configuration information that it needs in order to send notification information to the FPolicy servers. It specifies the primary servers and secondary servers to which the cluster will send notifications. It also specifies FPolicy server related configuration information.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy external engine.

---

**-engine-name** <Engine name> - Engine

This parameter specifies the name of the FPolicy external engine that you want to create. An external engine name can be up to 256 characters long. An external engine name is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_", and ".".

**-primary-servers** <IP Address>, ... - Primary FPolicy Servers

This parameter specifies a list of IP addresses for the primary FPolicy servers to which you want the external engine you create to apply. The `-primary-servers` parameter is used to specify a list of servers to which to send file access events for a given FPolicy policy. When an administrator configures multiple servers as primary servers, notifications are sent to the FPolicy servers in a round-robin fashion.

**-port** <integer> - Port Number of FPolicy Service

This parameter specifies the port number for the FPolicy service.

**[-secondary-servers** <IP Address>, ...] - Secondary FPolicy Servers

This parameter specifies a list of IP addresses for the secondary FPolicy servers to which you want the external engine you create to apply. Secondary servers will be used only when all the primary servers are not reachable. When an administrator configures multiple servers as secondary servers, notifications are sent to FPolicy server in a round-robin fashion. By default, no secondary server is selected.

**[-extern-engine-type** <External Engine Type>] - External Engine Type

This parameter specifies the type of the external engine. This specifies how the FPolicy server should behave, synchronously or asynchronously. By default, it is synchronous in nature. When set to synchronous, after sending a notification to the external FPolicy server, request processing does not continue until after receiving a response from the FPolicy server. At that point request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to asynchronous, after sending a notification to the external FPolicy server, file request processing continues.

**-ssl-option** {no-auth|server-auth|mutual-auth} - SSL Option for External Communication

This parameter specifies the SSL option for external communication with the FPolicy server. Possible values include the following:

- **no-auth** : When set to no-auth, no authentication takes place. The communication link is established over the TCP protocol.
- **server-auth** : When set to server-auth, only the FPolicy server is authenticated by the Vserver. With this option, before creating the FPolicy external engine, the

---

administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

- **mutual-auth** : When set to mutual-auth, mutual authentication takes place between the Vserver and the FPolicy server, i.e. authentication of the FPolicy server by the Vserver along with authentication of the Vserver by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the Vserver.

The public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate is installed using the `security certificate install` command with `-type` set to `client_ca`. The private key and public certificate required for authentication of the Vserver is installed using the `security certificate install` command with `-type` set to `server`.

**[-reqs-cancel-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Canceling a Request (privilege: advanced)

This parameter specifies the timeout for canceling a request. It is used to specify the time interval in which the node waits for a response from the FPolicy server. Beyond this timeout, a cancel request is sent to the FPolicy server to cancel the pending request. The request is then sent to an alternate FPolicy server that is registered for the policy. This timeout helps in handling a FPolicy server that is not responding, which can improve CIFS/NFS client response. Also, this feature can help in releasing of system resources since the request is moved from a down/bad FPolicy server to an alternate FPolicy server. The value for this field must be between 0s and 100s. By default, it is 20s.

**[-reqs-abort-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Aborting a Request (privilege: advanced)

This parameter specifies the timeout for aborting a request. The value for this field must be between 0s and 200s. By default, it is 40s.

**[-status-req-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Status Requests (privilege: advanced)

This parameter specifies the interval for sending status requests. It is used to specify the interval after which a status request will be send to the FPolicy server. The value for this field must be between 0s and 50s. By default, it is 10s.

**[-max-connection-retries <integer>]** - Max Reconnect Attempt (privilege: advanced)

---

This parameter specifies the maximum number of attempts to reconnect to the FPolicy server from a Vserver. It is used to specify the number of times a broken connection will be retried. The value for this field must be between 0 and 20. By default, it is 5.

**[-max-server-reqs <integer>]** - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

This parameter specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. By default, it is 50.

**[-server-progress-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

This parameter specifies the timeout for disconnecting non-responsive FPolicy servers. It is used to specify the time interval after which the connection to the FPolicy server is terminated. This happens only when the FPolicy server's queue contains the maximum allowed number of requests that it can hold in its queue and no response is received within this timeout. The maximum allowed number of requests is either 50 (the default) or the number specified by the `-max-server-reqs` parameter. The value for this field must be between 1s and 100s. By default, it is 60s.

**[-keep-alive-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Keep-Alive Messages (privilege: advanced)

This parameter specifies the interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages are used to detect half-open connections. The range of supported values for this field is 10 through 600 (h, m, or s). Alternatively, the value can be set to 0, which disables keep-alive messages and prevents them from being sent to the FPolicy servers. The default value for this field is 120s.

**[-certificate-common-name <FQDN or Custom Common Name>]** - FQDN or Custom Common Name

This parameter specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the Vserver and the FPolicy server is configured.

**[-certificate-serial <text>]** - Serial Number of Certificate

This parameter specifies the serial number of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

**[-certificate-ca <text>]** - Certificate Authority

---

This parameter specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

## Examples

The following example creates an FPolicy external engine.

```
Cluster::> vsriver fpolicy policy external-engine create -vserver vs1 -engine-
name new_engine -primary-servers 1.1.1.1 -port 10 -secondary-servers 2.2.2.2
-ssl-option mutual-auth -extern-engine-type synchronous -certificate-serial
8DDE112A114D1FBC -certificate-common-name Sample1-FPolicy-Client -certificate-ca
TASample1

Cluster::> vsriver fpolicy policy external-engine show -vserver vs1 -engine-name
new_engine

Vserver: vs1
Engine: new_engine
Primary FPolicy Servers: 1.1.1.1
Port Number of FPolicy Service: 10
Secondary FPolicy Servers: 2.2.2.2
External Engine Type: synchronous
SSL Option for External Communication: mutual-auth
FQDN or Custom Common Name: Sample1-FPolicy-Client
Serial Number: 8DDE112A114D1FBC
Certificate Authority: TASample1
```

## See Also

security certificate install

---

## vserver fpolicy policy external-engine delete

Delete an external engine

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy external-engine delete` command deletes an FPolicy external engine.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to delete an FPolicy external engine.

**-engine-name** <Engine name> - Engine

This parameter specifies the name of the FPolicy external engine you want to delete.

### Examples

The following example deletes an FPolicy external engine.

```
Cluster::> vserver fpolicy policy external-engine show -vserver vs1 -engine-name
new_engine
      Vserver: vs1
      Engine: new_engine
      Primary FPolicy Servers: 1.1.1.1
Port Number of FPolicy Service: 10
      Secondary FPolicy Servers: 2.2.2.2
      External Engine Type: synchronous
SSL Option for External Communication: mutual-auth
      FQDN or Custom Common Name: Sample1-FPolicy-Client
      Serial Number: 8DDE112A114D1FBC
      Certificate Authority: TASample1

Cluster::>vserver fpolicy policy external-engine delete -vserver vs1 -engine-name
new_engine
```

---

## vserver fpolicy policy external-engine modify

Modify an external engine

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy external-engine modify` command modifies an FPolicy external engine. The cluster uses the external engine to hold configuration information that it needs in order to send notification information to the FPolicy servers. It specifies the primary servers and secondary servers to which the cluster will send notifications. It also specifies FPolicy server related configuration information.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy external engine.

**-engine-name** <Engine name> - Engine

This parameter specifies the name of the FPolicy external engine that you want to modify. An external engine name can be up to 256 characters long. An external engine name is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "\_", and ".".

**[-primary-servers** <IP Address>, ...] - Primary FPolicy Servers

This parameter specifies a list of IP addresses for the primary FPolicy servers to which you want the external engine you modify to apply. The `-primary-servers` parameter is used to specify a list of servers to which to send file access events for a given FPolicy policy. When an administrator configures multiple servers as primary servers, notifications are sent to the FPolicy servers in a round-robin fashion.

**[-port** <integer>] - Port Number of FPolicy Service

This parameter specifies the port number for the FPolicy service.



---

**[-secondary-servers <IP Address>, ...] - Secondary FPolicy Servers**

This parameter specifies a list of IP addresses for the secondary FPolicy servers to which you want the external engine you modify to apply. Secondary servers will be used only when all the primary servers are not reachable. When an administrator configures multiple servers as secondary servers, notifications are sent to FPolicy server in a round-robin fashion. By default, no secondary server is selected.

**[-extern-engine-type <External Engine Type>] - External Engine Type**

This parameter specifies the type of the external engine. This specifies how the FPolicy server should behave, synchronously or asynchronously. By default, it is synchronous in nature. When set to synchronous, after sending a notification to the external FPolicy server, request processing does not continue until after receiving a response from the FPolicy server. At that point request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to asynchronous, after sending a notification to the external FPolicy server, file request processing continues.

**[-ssl-option {no-auth|server-auth|mutual-auth}] - SSL Option for External Communication**

This parameter specifies the SSL option for external communication with the FPolicy server. Possible values include the following:

- **no-auth** : When set to no-auth, no authentication takes place. The communication link is established over the TCP protocol.
- **server-auth** : When set to server-auth, only the FPolicy server is authenticated by the Vserver. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.
- **mutual-auth** : When set to mutual-auth, mutual authentication takes place between the Vserver and the FPolicy server, i.e. authentication of the FPolicy server by the Vserver along with authentication of the Vserver by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the Vserver.

The public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate is installed using the `security certificate install` command with `-type` set to `client_ca`. The private key and public certificate required for authentication of the Vserver is installed using the `security certificate install` command with `-type` set to `server`.

---

**[-reqs-cancel-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Canceling a Request (privilege: advanced)

This parameter specifies the timeout for canceling a request. It is used to specify the time interval in which the node waits for a response from the FPolicy server. Beyond this timeout, a cancel request is sent to the FPolicy server to cancel the pending request. The request is then sent to an alternate FPolicy server that is registered for the policy. This timeout helps in handling a FPolicy server that is not responding, which can improve CIFS/NFS client response. Also, this feature can help in releasing of system resources since the request is moved from a down/bad FPolicy server to an alternate FPolicy server. The value for this field must be between 0s and 100s. By default, it is 20s.

**[-reqs-abort-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Aborting a Request (privilege: advanced)

This parameter specifies the timeout for aborting a request. The value for this field must be between 0s and 200s. By default, it is 40s.

**[-status-req-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Status Requests (privilege: advanced)

This parameter specifies the interval for sending status requests. It is used to specify the interval after which a status request will be send to the FPolicy server. The value for this field must be between 0s and 50s. By default, it is 10s.

**[-max-connection-retries <integer>]** - Max Reconnect Attempt (privilege: advanced)

This parameter specifies the maximum number of attempts to reconnect to the FPolicy server from a Vserver. It is used to specify the number of times a broken connection will be retried. The value for this field must be between 0 and 20. By default, it is 5.

**[-max-server-reqs <integer>]** - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

This parameter specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify the maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. By default, it is 50.

**[-server-progress-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

This parameter specifies the timeout for disconnecting non-responsive FPolicy servers. It is used to specify the time interval after which the connection to the FPolicy server is terminated. This happens only when the FPolicy server's queue contains the maximum allowed number of requests that it can hold in its queue and no response is received within this timeout. The maximum allowed number of requests is either 50 (the default)

---

or the number specified by the `-max-server-reqs` parameter. The value for this field must be between 1s and 100s. By default, it is 60s.

**[-keep-alive-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Keep-Alive Messages (privilege: advanced)

This parameter specifies the interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages are used to detect half-open connections. The range of supported values for this field is 10 through 600 (h, m, or s). Alternatively, the value can be set to 0, which disables keep-alive messages and prevents them from being sent to the FPolicy servers. The default value for this field is 120s.

**[-certificate-common-name <FQDN or Custom Common Name>]** - FQDN or Custom Common Name

This parameter specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the Vserver and the FPolicy server is configured.

**[-certificate-serial <text>]** - Serial Number of Certificate

This parameter specifies the serial number of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

**[-certificate-ca <text>]** - Certificate Authority

This parameter specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

## Examples

The following example modifies an FPolicy external engine.

```
Cluster::> vsriver fpolicy policy external engine modify -vsriver vs1 -engine-  
name new_engine -primary-servers 1.1.1.1 -port 10 -secondary-servers 2.2.2.2
```

```
Cluster::> vsriver fpolicy policy external-engine show -vsriver vs1 -engine-name  
new_engine
```

```
                Vserver: vs1  
                Engine: new_engine  
    Primary FPolicy Servers: 1.1.1.1  
Port Number of FPolicy Service: 10  
    Secondary FPolicy Servers: 2.2.2.2  
    External Engine Type: synchronous  
SSL Option for External Communication: mutual-auth  
    FQDN or Custom Common Name: Sample1-FPolicy-Client  
                Serial Number: 8DDE112A114D1FBC  
    Certificate Authority: TASample1
```

## See Also

---

security certificate install

---

## vserver fpolicy policy external-engine show

Display external engines

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy external-engine show` command displays information about all FPolicy external engines belonging to the Vserver. Any Vserver administrator can see FPolicy external engines associated to their Vserver as well as external engines created by cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy external engines:

- Vserver name
- FPolicy external engine name
- List of primary FPolicy servers
- List of secondary FPolicy servers
- Port number for FPolicy service
- FPolicy external engine type

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy external engines. You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about all external engines where the `-port` parameter is set to 9, run the command with the `-field` parameter set to `engine-name` and `-port` parameter set to 9.

You can specify the `-instance` parameter to display all information for all policies in a list format.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]

---

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information only about the FPolicy external engines for the specified Vserver. Cluster administrator created FPolicy external engines are visible in all Vserver.

**[-engine-name <Engine name>]** - Engine

If you specify this parameter, the command displays information only about the FPolicy external engine that you specify.

**[-primary-servers <IP Address>, ...]** - Primary FPolicy Servers

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified IP addresses as primary FPolicy servers.

**[-port <integer>]** - Port Number of FPolicy Service

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified port for the FPolicy service.

**[-secondary-servers <IP Address>, ...]** - Secondary FPolicy Servers

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified IP addresses as secondary FPolicy servers.

**[-extern-engine-type <External Engine Type>]** - External Engine Type

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified external engine type.

**[-ssl-option {no-auth|server-auth|mutual-auth}]** - SSL Option for External Communication

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified ssl option.

**[-reqs-cancel-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Canceling a Request (privilege: advanced)

---

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for canceling a request.

**[-reqs-abort-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Aborting a Request (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for aborting a request.

**[-status-req-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Status Requests (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified interval for sending status requests.

**[-max-connection-retries <integer>]** - Max Reconnect Attempt (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified maximum reconnect attempts.

**[-max-server-reqs <integer>]** - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified FPolicy server maximum outstanding requests.

**[-server-progress-timeout <[<integer>h][<integer>m][<integer>s]>]** - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for disconnecting non-responsive server.

**[-keep-alive-interval <[<integer>h][<integer>m][<integer>s]>]** - Interval for Sending Keep-Alive Messages (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified keep-alive interval.

**[-certificate-common-name <FQDN or Custom Common Name>]** - FQDN or Custom Common Name

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate common name.

**[-certificate-serial <text>]** - Serial Number of Certificate

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate serial number.

---

## **[-certificate-ca <text>] - Certificate Authority**

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate authority name.

## **Examples**

The following example displays the information about the configured external engines using the `vserver fpolicy policy external-engine show` command.

```
Cluster::>vserver fpolicy policy external-engine show
Vserver      Engine      Primary      Secondary      External
-----      -
Cluster      cserver_eng  9.9.9.9      -              9 synchronous
vs1          cserver_eng  9.9.9.9      -              9 synchronous
vs1          vn1         1.1.1.1      2.2.2.2        1 synchronous
vs2          cserver_eng  9.9.9.9      -              9 synchronous
vs2          v2n1        3.3.3.3      5.5.5.5        2 synchronous
5 entries were displayed.
```

The following example displays the information about all Vserver FPolicy external engines with the `-port` parameter set to 9.

```
Cluster::> vserver fpolicy policy external-engine show -fields engine-name -port
9
vserver engine-name
-----
Cluster cserver_eng
vs1     cserver_eng
vs2     cserver_eng
3 entries were displayed.
```



---

## vserver fpolicy policy scope create

Create scope

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy scope create` command creates an FPolicy scope for an FPolicy policy. A scope defines the boundaries on which the FPolicy policy will apply. The Vserver is the basic scope boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply and you must designate to which Vserver you want to apply the scope. There are a number of parameters that further restrict the scope within the specified Vserver. You can restrict the scope by specifying what to include in the scope. Or you can restrict the scope by specifying what to exclude from the scope. For example, you can restrict the scope by specifying which volumes to include using the `-volumes-to-include` parameter or which volumes to exclude using the `-volumes-to-exclude` parameter. Once you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Note:

There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin Vserver. If the cluster administrator also creates the scope for that cluster FPolicy policy, a Vserver administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any Vserver administrator can create the scope for that cluster policy. In the event that the Vserver administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

---

This parameter specifies the name of the Vserver on which you want to create an FPolicy policy scope.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy for which you want to create the scope.

**[-shares-to-include** <Share name>, ...] - Shares to Include

This parameter specifies a list of shares for file access monitoring. With this option, the administrator provides a list of shares, separated by commas. For file access events relative to the specified shares and file operations monitored by the FPolicy policy, a notification is generated. The `-shares-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

Note:

When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.

**[-shares-to-exclude** <Share name>, ...] - Shares to Exclude

This parameter specifies a list of shares to exclude from file access monitoring. With this option, the administrator provides a list of shares, separated by commas. When a share is specified in the `-shares-to-exclude` parameter, no notification is sent for files accessed relative to that share. The `-shares-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**[-volumes-to-include** <volume name>, ...] - Volumes to Include

This parameter specifies a list of volumes for file access monitoring. With this option, the administrator provides a list of volumes, separated by commas. For file access events within the volume and file operations monitored by the FPolicy policy, a notification is generated. The `-volumes-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**[-volumes-to-exclude** <volume name>, ...] - Volumes to Exclude

This parameter specifies a list of volumes to exclude from file access monitoring. With this option, the administrator provides a list of volumes, separated by commas, for which no file access notifications are generated. The `-volumes-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

Note:

---

When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`. Similarly, when an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export-policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.

**`[-export-policies-to-include <FPolicy export policy>, ...]` - Export Policies to Include**

This parameter specifies a list of export policies for file access monitoring. With this option, the administrator provides a list of export policies, separated by commas. For file access events within an export policy and file operations monitored by the FPolicy policy, a notification is generated. The `-export-policies-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

Note:

When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.

**`[-export-policies-to-exclude <FPolicy export policy>, ...]` - Export Policies to Exclude**

This parameter specifies a list of export policies to exclude from file access monitoring. With this option, the administrator provides a list of export policies, separated by commas, for which no file access notification is sent. The `-export-policies-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**`[-file-extensions-to-include <File extension>, ...]` - File Extensions to Include**

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing is required. Any file access to files with the same extensions included in the `-file-extensions-to-include` parameter generates a notification. The `-file-extensions-to-include` parameter can contain regular expressions and can include metacharacters such as "?".

**`[-file-extensions-to-exclude <File extension>, ...]` - File Extensions to Exclude**

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing will be excluded. Using the exclude list, the administrator can request notification for all extensions except those in the excluded list. Any file access to files with the same extensions included in the `-file-extensions-to-exclude` parameter does not generate a notification. The `-file-`

extensions-to-exclude parameter can contain regular expressions and can include metacharacters such as "?".

Note:

An administrator can specify both -file-extensions-to-include and -file-extensions-to-exclude lists. The -file-extensions-to-exclude parameter is checked first before the -file-extensions-to-include parameter is checked.

**[-is-file-extension-check-on-directories-enabled {true|false}]** - Is File Extension Check on Directories Enabled (privilege: advanced)

This parameter specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to true, the directory objects are subjected to same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications would be sent for directories even if their name extensions do not match.

## Examples

The following example creates an FPolicy policy scope.

```
Cluster::>vserver fpolicy policy scope create -vserver vs1 -policy-
name vs1_pol                                -file-extensions-to-
include flv,wmv,mp3,mp4                      -file-extensions-to-
exclude cpp,c,h,txt
```

	Cluster::>vserver	fpolicy policy scope show		
	Vserver	Policy	Extensions	Extensions
	Name	Name	Included	Excluded
	-----			
	Cluster	cserver_pol	txt	mp3, wmv
txt	vs1	vs1_pol	flv, wmv, mp3, mp4	cpp, c, h,
	2 entries were displayed.			

---

## vserver fpolicy policy scope delete

Delete scope

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy scope delete` command deletes an FPolicy policy scope.

Note:

This command is not supported for a Vserver with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete the FPolicy policy scope.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy for which you want to delete the scope.

### Examples

The following example deletes a scope of an FPolicy policy.

```
Cluster::>vserver fpolicy policy scope delete -vserver vs1 -policy-name  
vs1_pol
```

## vserver fpolicy policy scope modify

Modify scope

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver fpolicy policy scope modify` command modifies an FPolicy scope for an FPolicy policy. A scope defines the boundaries on which the FPolicy policy will apply. The Vserver is the basic scope boundary. When you modify a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply and you must designate to which Vserver you want to apply the scope. There are a number of parameters that further restrict the scope within the specified Vserver. You can restrict the scope by specifying what to include in the scope. Or you can restrict the scope by specifying what to exclude from the scope. For example, you can restrict the scope by specifying which volumes to include using the `-volumes-to-include` parameter or which volumes to exclude using the `-volumes-to-exclude` parameter. Once you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Note:

This command is not supported for a Vserver with Infinite Volume.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy policy scope.

**-policy-name** <Policy name> - Policy

This parameter specifies the name of the FPolicy policy for which you want to modify the scope.

**[-shares-to-include** <Share name>, ...] - Shares to Include

This parameter specifies a list of shares for file access monitoring. With this option, the administrator provides a list of shares, separated by commas. For file access events relative to the specified shares and file operations monitored by the FPolicy policy, a notification is generated. The `-shares-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

Note:

When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.

---

**[`-shares-to-exclude` <Share name>, ...] - Shares to Exclude**

This parameter specifies a list of shares to exclude from file access monitoring. With this option, the administrator provides a list of shares, separated by commas. When a share is specified in the `-shares-to-exclude` parameter, no notification is sent for files accessed relative to that share. The `-shares-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**[`-volumes-to-include` <volume name>, ...] - Volumes to Include**

This parameter specifies a list of volumes for file access monitoring. With this option, the administrator provides a list of volumes, separated by commas. For file access events within the volume and file operations monitored by the FPolicy policy, a notification is generated. The `-volumes-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**[`-volumes-to-exclude` <volume name>, ...] - Volumes to Exclude**

This parameter specifies a list of volumes to exclude from file access monitoring. With this option, the administrator provides a list of volumes, separated by commas, for which no file access notifications are generated. The `-volumes-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**Note:**

When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`. Similarly, when an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export-policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.

**[`-export-policies-to-include` <FPolicy export policy>, ...] - Export Policies to Include**

This parameter specifies a list of export policies for file access monitoring. With this option, the administrator provides a list of export policies, separated by commas. For file access events within an export policy and file operations monitored by the FPolicy policy, a notification is generated. The `-export-policies-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "\*".

**Note:**

When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.

---

**[-export-policies-to-exclude <FPolicy export policy>, ...]** - Export Policies to Exclude

This parameter specifies a list of export policies to exclude from file access monitoring. With this option, the administrator provides a list of export policies, separated by commas, for which no file access notification is sent. The `-export-policies-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and \*.

**[-file-extensions-to-include <File extension>, ...]** - File Extensions to Include

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing is required. Any file access to files with the same extensions included in the `-file-extensions-to-include` parameter generates a notification. The `-file-extensions-to-include` parameter can contain regular expressions and can include metacharacters such as "?".

**[-file-extensions-to-exclude <File extension>, ...]** - File Extensions to Exclude

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing will be excluded. Using the exclude list, the administrator can request notification for all extensions except those in the excluded list. Any file access to files with the same extensions included in the `-file-extensions-to-exclude` parameter does not generate a notification. The `-file-extensions-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?".

Note:

An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists. The `-file-extensions-to-exclude` parameter is checked first before the `-file-extensions-to-include` parameter is checked.

**[-is-file-extension-check-on-directories-enabled {true|false}]** - Is File Extension Check on Directories Enabled (privilege: advanced)

This parameter specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to true, the directory objects are subjected to same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications would be sent for directories even if their name extensions do not match.

## Examples

The following example modifies an FPolicy policy scope.

```
Cluster::>vserver fpolicy policy scope modify -vserver vs1 -policy-  
name vs1_pol
```



```
include flv,wmv,mp3,mp4                                     -file-extensions-to-
exclude cpp,c,h,txt                                         -file-extensions-to-

Cluster::>vserver fpolicy policy scope show
Vserver          Policy          Extensions          Extensions
Name             Name             Included            Excluded
-----
Cluster          cserver_pol          txt                mp3, wmv
vsl              vsl_pol            flv, wmv, mp3, mp4  cpp, c, h,
txt              2 entries were displayed.
```

---

## vserver fpolicy policy scope show

Display scope

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver fpolicy policy scope show` command displays scope information about all FPolicy policies belonging to the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy scopes:

- Vserver name
- Policy name
- The file extensions to include
- The file extensions to exclude

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy scopes. In addition to the fields above, you can display the following fields:

- The shares to include
- The shares to exclude
- The volumes to include
- The volumes to exclude
- The export policies to include
- The export policies to exclude
- Whether file extension check on directories is enabled

You can specify specific parameters to display only information that matches those parameters. For example, to display scope information only about all FPolicy policies where the `-file-extensions-to-include` parameter is set to `txt`, run the command with the `-fields` parameter set to `policy-name` and `-file-extensions-to-include` parameter set to `txt`.

---

You can specify the `-instance` parameter to display scope information for all FPolicy policies in a list format.

Note:

This command is not supported for a Vserver with Infinite Volume.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays scope information only about the FPolicy policies for the specified Vserver.

**[-policy-name <Policy name>]** - Policy

If you specify this parameter, the command displays information only about the specified FPolicy policy.

**[-shares-to-include <Share name>, ...]** - Shares to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified share or shares in the include list.

**[-shares-to-exclude <Share name>, ...]** - Shares to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified share or shares in the exclude list.

**[-volumes-to-include <volume name>, ...]** - Volumes to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified volume or volumes in the include list.

**[-volumes-to-exclude <volume name>, ...]** - Volumes to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified volume or volumes in the exclude list.

**[-export-policies-to-include <FPolicy export policy>, ...]** - Export Policies to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified export policy or policies in the include list.

**[-export-policies-to-exclude <FPolicy export policy>, ...]** - Export Policies to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified export policy or policies in the exclude list.

**[-file-extensions-to-include <File extension>, ...]** - File Extensions to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension or extensions in the include list.

**[-file-extensions-to-exclude <File extension>, ...]** - File Extensions to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension or extensions in exclude list.

**[-is-file-extension-check-on-directories-enabled {true|false}]** - Is File Extension Check on Directories Enabled (privilege: advanced)

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension check on directories. If set to true, the command displays information about scopes where file extension checks on directories is enabled. If set to false, the command displays information about scopes where file extension checks on directories is disabled.

## Examples

The following example displays scope information about FPolicy policies.

```
Cluster::>vserver fpolicy policy scope show
Vserver          Policy          Extensions          Extensions
Name             Name             Included            Excluded
-----
Cluster          cserver_pol      -                   -
vs1              p                 -                   -
vs1              vs1_pol          mp3                 -
3 entries were displayed.
```

---

## vserver group-mapping create

Create a group mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver group-mapping create` command creates a group mapping. Group mappings are applied in the order in which they occur in the priority list; for example, a group mapping that occurs at position 2 in the priority list is applied before a group mapping that occurs at position 3. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list. Data ONTAP prevents you from creating two group mappings with the same pattern.

Patterns can be expressed as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 group mappings in each direction.

The `vserver group-mapping create` command is not supported on Vservers with FlexVol volumes.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression `(.+)` in the CLI, type `"(.+)"` at the command prompt. To add a `"?"` to the expression, press ESC followed by the `"?"`.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to create the group mapping.

**-direction** <Direction of the name mapping> - Group Mapping Direction

This parameter specifies the direction of the group mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX group mapping, `win-unix` for a Windows-to-UNIX group mapping, and `unix-win` for a UNIX-to-Windows group mapping.

**-position** <integer> - Position

This parameter specifies the group mapping's position in the priority list. Specify the position as a positive integer.

---

## Note:

If you want to create a new group mapping at a position that is already occupied in the priority list, use the `vserver group-mapping insert` command instead of the `vserver group-mapping create` command.

### **-pattern <text>** - Pattern

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

### **-replacement <text>** - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.

## Examples

The following example creates a group mapping on a Vserver named `vs1`. The mapping is from UNIX to Windows at position 5 in the priority list. The mapping maps the pattern `cifs` to the replacement `EXAMPLE\Domain Groups`.

```
cluster1::> vserver group-mapping create -vserver vs1 -direction unix-win -  
position 5 -pattern cifs -replacement "EXAMPLE\Domain Groups"
```

## See Also

`vserver group-mapping insert`

---

## vserver group-mapping delete

Delete a group mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver group-mapping delete` command deletes a group mapping.

The `vserver group-mapping delete` command is not supported on Vservers with FlexVol volumes.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to delete the group mapping.

**-direction** <Direction of the name mapping> - Group Mapping Direction

This parameter specifies the direction of the group mapping that you want to delete.

**-position** <integer> - Position

This parameter specifies the position of the group mapping that you want to delete. Specify the position as a positive integer.

### Examples

The following example deletes a group mapping on a Vserver named `vs1`. The group mapping is from UNIX to Windows and is at position 5.

```
cluster1::> vserver group-mapping delete -vserver vs1 -direction unix-win -  
position 5
```

## vserver group-mapping insert

Create a group mapping at a specified position

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

---

The `vserver group-mapping insert` command creates a group mapping at a specified position in the priority list. The command rearranges the list as needed to accommodate the new entry. For instance, if you have a priority list of five mappings and insert a new mapping at position 3, the mapping previously at position 3 is moved to position 4, the mapping previously at position 4 is moved to position 5, and the mapping previously at position 5 is moved to position 6. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

You can specify patterns as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 group mappings in each direction.

The `vserver group-mapping insert` command is not supported on Vservers with FlexVol volumes.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression `(.+)` in the CLI, type `"(.+)"` at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

## Parameters

**-vserver** <vserver> - Vserver

This parameter specifies the Vserver on which you want to create the group mapping.

**-direction** <Direction of the name mapping> - Group Mapping Direction

This parameter specifies the direction of the group mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX group mapping, `win-unix` for a Windows-to-UNIX group mapping, and `unix-win` for a UNIX-to-Windows group mapping.

**-position** <integer> - Position

This parameter specifies the position in the priority list at which you want to insert the new group mapping. Specify a position as a positive integer.

**-pattern** <text> - Pattern

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

**-replacement** <text> - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.



---

## Examples

The following example creates a group mapping on a Vserver named vs1. It is a group mapping from Kerberos to UNIX. It is inserted into the priority list at position 2. The group mapping maps any principal in the Kerberos realm SEC.EXAMPLE.COM to the UNIX group name corresponding to the principal's base name with any instance names removed; for example, artists/admin@SEC.EXAMPLE.COM is mapped to artists.

```
cluster1::> vserver group-mapping insert -vserver vs1 -direction krb-unix -  
position 2 -pattern "([^\@/]+)(/[^\@]+)?@SEC.EXAMPLE.COM" -replacement "\1"
```

## vserver group-mapping modify

Modify a group mapping's pattern, replacement pattern, or both

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver group-mapping modify` command modifies the pattern, the replacement pattern, or both of a specified group mapping.

You can specify patterns as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 group mappings in each direction.

The `vserver group-mapping modify` command is not supported on Vservers with FlexVol volumes.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression (.+) in the CLI, type "(.+)\" at the command prompt. To add a "\"" to the expression, press ESC followed by the "?".

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to modify the group mapping.

**-direction** <Direction of the name mapping> - Group Mapping Direction

---

This parameter specifies the direction of the group mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX group mapping, `win-unix` for a Windows-to-UNIX group mapping, and `unix-win` for a UNIX-to-Windows group mapping.

**-position** <integer> - Position

This parameter specifies the group mapping's position in the priority list. A position is specified as a positive integer. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

**[-pattern** <text>] - Pattern

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

**[-replacement** <text>] - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.

## Examples

The following example modifies the group mapping on the Vserver named `vs1` and direction `win-unix`, at position 3. The pattern to be matched is changed to `"EXAMPLE\(.+)"`.

```
cluster1::> vsserver group-mapping modify -vsserver vs1 -direction win-unix -  
position 3 -pattern "EXAMPLE\(.+)"
```

## vserver group-mapping show

Display group mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver group-mapping show` command displays information about group mappings. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all group mappings:

- Vserver name
- Direction of the mapping (`krb-unix` for Kerberos-to-UNIX, `win-unix` for Windows-to-UNIX, or `unix-win` for UNIX-to-Windows)

- 
- Position of the mapping in the priority list
  - Pattern to be matched
  - Replacement pattern

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about Kerberos-to-UNIX group mappings, run the command with the `-direction krb-unix` parameter.

The `vserver group-mapping show` command is not supported on Vservers with FlexVol volumes.

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the group mapping or mappings that match the specified Vserver.

[-direction <Direction of the name mapping>] - Group Mapping Direction

If you specify this parameter, the command displays information only about the group mapping or mappings that have the specified mapping direction.

[-position <integer>] - Position

If you specify this parameter, the command displays information only about the group mapping that has the specified position in the priority list.

[-pattern <text>] - Pattern

If you specify this parameter, the command displays information only about the group mapping or mappings that use the specified matching pattern. The pattern can be up to 256 characters in length. Refer to the command description section for details.

[-replacement <text>] - Replacement

---

If you specify this parameter, the command displays information only about the group mapping or mappings that use the specified replacement pattern.

### Examples

The following example displays information about all group mappings:

```
cluster1::> vserver group-mapping show
Vserver      Direction Position
-----
vs1          win-unix  1      Pattern: EXAMPLE\\artists
            Replacement: nobody
vs1          unix-win  1      Pattern: EXAMPLE\\(.+)
            Replacement: \_1
vs2          win-unix  1      Pattern: (.+)
            Replacement: EXAMPLE\\artists
```

---

## vserver group-mapping swap

Exchange the positions of two group mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver group-mapping swap` command exchanges the positions of two group mappings in the priority list.

The `vserver group-mapping swap` command is not supported on Vservers with FlexVol volumes.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the group mappings are located.

**-direction** <Direction of the name mapping> - Group Mapping Direction

This parameter specifies the direction of the group mappings that you want to exchange. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

**-position** <integer> - Position

This parameter specifies the position in the priority list of the first group mapping that you want to exchange. Specify a position as a positive integer.

**-with-position** <integer> - Position of an existing group mapping entry in the list of group mappings for this Vserver. This entry will be swapped with the entry at 'position'.

This parameter specifies the position in the priority list of the second group mapping that you want to exchange. Specify a position as a positive integer.

### Examples

The following example exchanges the positions of two group mappings on a Vserver named `vs1`. The group mappings have the direction `Windows-to-UNIX`. The group mappings are exchanged between positions 2 and 4.

```
cluster1::> vserver group-mapping swap -vserver vs1 -direction win-unix -position  
2 -with-position 4
```

---

## vserver iscsi create

Create a Vserver's iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates an iSCSI target for a specified Vserver. By default the system creates a default iSCSI target name with the status-admin set to enabled. Until you create an iSCSI service, iSCSI initiators cannot log into the Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the iSCSI service.

**[-target-name <text>]** - Target Name (privilege: advanced)

Specifies a iSCSI target name of a Vserver. This name is unique and is not case sensitive. The target name must conform to this format `iqn.1995-08.com.example:string` and follow these rules:

- Contains up to 223 bytes.
- Contains alphanumeric characters. The period ".", hyphen "-", and colon ":" are acceptable.
- Does not contain the underscore character "\_".

**[-target-alias <text>]** - Target Alias

Specifies an iSCSI target alias name of a Vserver. The maximum number of characters for an alias name is 128. The alias default name is the Vserver name.

**[-status-admin {down|up}]** - Administrative Status

Specifies the administrative status of the iSCSI service of a Vserver. If you set this parameter to up, the command creates an iSCSI service with the administrative status of up. If you set this parameter to down, the command creates an iSCSI service with the administrative status of down.

**[-max-error-recovery-level <integer>]** - Max Error Recovery Level (privilege: advanced)

---

Specifies the maximum error recovery level allowed by the iSCSI service. You can specify 0, 1, or 2, or you can accept the default. The default is zero. The actual error recovery level depends on the negotiated error recovery level between the initiator and the iSCSI target when the session is created.

- 0 - Session failure recovery
- 1 - Digest failure recovery
- 2 - Connection failure recovery

**[-retain-timeout <integer>]** - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Specifies the wait time before an active task reassignment is possible after an unexpected connection termination. For example, a value of 0 means that the connection or task state is immediately discarded by the target. The default is 20 seconds.

**[-login-timeout <integer>]** - Login Phase Duration (in sec) (privilege: advanced)

Specifies the login phase duration. The default is 15 seconds.

**[-max-conn-per-session <integer>]** - Max Connections per Session (privilege: advanced)

Specifies the maximum number of connections per session that a target can accept. The default is 4 connections.

**[-max-ios-per-session <integer>]** - Max Commands per Session (privilege: advanced)

Specifies the maximum number of commands per session that a target can accept. The default is 128 commands per session.

**[-tcp-window-size <integer>]** - TCP Receive Window Size (in bytes) (privilege: advanced)

Specifies the TCP receive window size (in bytes). The default is 131,400 bytes.

**[-force | -f [true]]** - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

## Examples

```
cluster:::> vservice iscsi create -vservice vs_1
```

Creates the iSCSI service for Vservice vs\_1.

---

## vserver iscsi delete

Delete a Vserver's iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command deletes the iSCSI service from a Vserver.

Note:

You must first disable the service with the command `vserver iscsi modify` with "status-admin down" before you can delete the service.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the iSCSI service.

### Examples

```
cluster::> vserver iscsi delete -vserver vs_1
```

Deletes the iSCSI service for Vserver vs\_1.

### See Also

`vserver iscsi modify`



---

## vserver iscsi modify

Modify a Vserver's iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command modifies the configuration for an iSCSI service.

Modifications take effect immediately after you execute the command. Making modifications to your service can result in traffic loss on a live system. Call technical support if you are unsure of the possible consequences.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the iSCSI service.

**[-target-name <text>]** - Target Name (privilege: advanced)

Specifies an iSCSI target name of a Vserver. This name is unique and is not case sensitive. The target name must conform to this format `iqn.1995-08.com.example:string` and follow these rules:

- Contains up to 223 bytes.
- Contains alphanumeric characters. The period ".", hyphen "-", and colon ":" are acceptable.
- Does not contain the underscore character "\_".

Note:

The iSCSI service must be down in order to change the target name.

**{ [-target-alias <text>] - Target Alias**

Specifies the new target alias of the iSCSI service.

**| [-clear | -c [true]] }** - Clear the Target Alias

Clears the current target alias from the iSCSI service configuration.

**[-status-admin {down|up}]** - Administrative Status

---

Specifies the configured administrative status of a service. If you set this parameter to up, the iSCSI service begins to accept login requests from iSCSI initiators. If you set this parameter to down, iSCSI initiators cannot log in.

**[-max-error-recovery-level <integer>]** - Max Error Recovery Level (privilege: advanced)

Specifies the maximum error recovery level the iSCSI service negotiates with iSCSI initiators during login phase.

- 0 - Session failure recovery
- 1 - Digest failure recovery
- 2 - Connection failure recovery

**[-retain-timeout <integer>]** - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Specifies the wait time before active task reassignment is possible after an unexpected connection termination. For example, a value of 0 means that the connection or task state is immediately discarded by the target.

**[-login-timeout <integer>]** - Login Phase Duration (in sec) (privilege: advanced)

Specifies maximum time the login phase remains active until the iSCSI target terminates the connection.

**[-max-conn-per-session <integer>]** - Max Connections per Session (privilege: advanced)

Specifies the maximum number of connections per session that the iSCSI target can accept.

**[-max-ios-per-session <integer>]** - Max Commands per Session (privilege: advanced)

Specifies the maximum number of commands per session that the iSCSI target can accept.

**[-tcp-window-size <integer>]** - TCP Receive Window Size (in bytes) (privilege: advanced)

Specifies the TCP receive window size (in bytes).

A change to the TCP receive window size value takes effect for all network interfaces when you restart the iSCSI service for the Vserver as follows:

```
vserver iscsi stop -vserver <vserver name>  
vserver iscsi start -vserver <vserver name>
```

If you change an individual network interface from up to down back to up, as follows, the new value for TCP receive window size takes effect for that network interface:

---

```
network interface modify -vserver <vserver name> -lif <LIF name> -status-admin  
down  
network interface modify -vserver <vserver name> -lif <LIF name> -status-admin up
```

**[-force | -f [true]]** - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

## Examples

```
cluster::> vserver iscsi modify -vserver vs_1 -status-admin down
```

Modifies the status-admin of the iSCSI service for Vserver vs\_1 to down.

## See Also

vserver iscsi stop   vserver iscsi start   network interface modify

---

## vserver iscsi show

Display a Vserver's iSCSI configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the current configuration of the iSCSI service.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Selects the iSCSI services for the Vserver that matches the parameter value.

[-**target-name** <text>] - Target Name (privilege: advanced)

Selects the iSCSI services with a target name that matches the parameter value.

[-**target-alias** <text>] - Target Alias

Selects the iSCSI services with a target alias that matches the parameter value.

[-**status-admin** {down|up}] - Administrative Status

Selects the iSCSI services with a configured status that matches the parameter value.

[-**max-error-recovery-level** <integer>] - Max Error Recovery Level (privilege: advanced)

Selects the iSCSI services with a maximum error recovery level that matches the parameter value.

[-**retain-timeout** <integer>] - RFC3720 DefaultTime2Retain Value (in sec) (privilege: advanced)

Selects the iSCSI services with a wait time that matches the parameter value. The wait time is the amount of time before active task reassignment is possible after an unexpected connection termination.

**[-login-timeout <integer>]** - Login Phase Duration (in sec) (privilege: advanced)

Selects the iSCSI services with a login phase duration that matches the parameter value.

**[-max-conn-per-session <integer>]** - Max Connections per Session (privilege: advanced)

Selects the iSCSI services with a maximum connection per session that matches the parameter value.

**[-max-ios-per-session <integer>]** - Max Commands per Session (privilege: advanced)

Selects the iSCSI services with a maximum number of commands per session that matches the parameter value.

**[-tcp-window-size <integer>]** - TCP Receive Window Size (in bytes) (privilege: advanced)

Selects the iSCSI services with a TCP receive window size (in bytes) that matches the parameter value.

## Examples

```
cluster::> vserver iscsi show
      Target                               Target                               Status
Vserver Name                               Alias                               Admin
-----
vs_1      iqn.1992-08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2  vs_1_alias  up
1 entries were displayed.
cluster::> vserver iscsi show -instance
```

```

      Vserver: vs_1
      Target Name:
iqn.1992-08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2 The following
is the output of the show command at the advanced privilege level:
      Target Alias: vs_1_alias
      Administrative Status: up
1 entries were displayed.
```

Displays the output of the show command at the admin privilege level.

```
cluster::*> vserver iscsi show
      Target                               Target                               Status
Vserver Name                               Alias                               Admin
-----
vs_1      iqn.1992-08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2  vs_1_alias  up
1 entries were displayed.
```

Displays the output of the show command at the advanced privilege level.

```
cluster::*> vserver iscsi show -instance
```

---

```

Vserver: vs_1
Target Name:
iqn.1992-08.com.example:sn.c7c82a22bf9f11df83e5123478563412:vs.2
Target Alias: vs_1_alias
Administrative Status: up
Max Error Recovery Level: 0
DefaultTime2Retain Value (in sec): 20
Login Phase Duration (in sec): 20
Max Connections per Session: 4
Max I/O per Session: 128
TCP Window Size all Sessions (in bytes): 131400
1 entries were displayed.
```

Displays the detailed entries for all entries.

---

## vserver iscsi start

Starts the iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command starts the iSCSI service of a Vserver. You can also use `vserver iscsi modify` with "-status-admin up".

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the iSCSI service.

### Examples

```
cluster::> vserver iscsi start -vserver vs_1
```

Starts the iSCSI service for Vserver vs\_1.

### See Also

`vserver iscsi modify`

---

## vserver iscsi stop

Stops the iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Stops the iSCSI service of a Vserver. This command shuts down all active iSCSI sessions and stops any new iSCSI sessions. You can also use `vserver iscsi modify` with "-status-admin down".

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver for the iSCSI service.

### Examples

```
cluster::> vserver iscsi stop -vserver vs_1
```

Stops the iSCSI service for Vserver vs\_1.

### See Also

`vserver iscsi modify`



---

## vserver iscsi command show

Display active iSCSI commands

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the status of active iSCSI commands in an iSCSI session. If you specify an iSCSI command ID, the command shows what commands are active in a session and is useful for initiator debugging.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display a list of active iSCSI commands that match the Vserver name that you specify.

[-**tpgroup** <text>] - Target Portal Group

Use this parameter to display a list of active iSCSI commands that are within the target portal group.

[-**tsih** <integer>] - Target Session ID

Use this parameter to display a list of active iSCSI commands that match the target session ID handle that you specify.

[-**command-id** <integer>] - Command ID

Use this parameter to display a list of active iSCSI commands that match the command ID that you specify.

[-**initiator-name** <text>] - Initiator Name

---

Use this parameter to display a list of active iSCSI commands that match the initiator name that you specify.

**[-initiator-alias <text>]** - Initiator Alias

Use this parameter to display a list of active iSCSI commands that match the initiator alias that you specify.

**[-isid <text>]** - Initiator Session ID

Use this parameter to display a list of active iSCSI commands that match the initiator session ID that you specify.

**[-command-sub-id <integer>]** - Command Sub ID

Use this parameter to display a list of active iSCSI commands that match the command sub ID that you specify.

**[-command-state <iSCSI Command States>]** - Command State

Use this parameter to display a list of active iSCSI commands that match the command state that you specify.

**[-command-type {Sequenced|Imm\_Taskmgmt|Imm\_Other}]** - Command Type

If you use this parameter, the command displays a list of active iSCSI commands that contains the specified command type. The command types indicate:

- "Sequenced" -- the system processes the commands in sequence
- "Imm\_Taskmgmt" -- the system processes the commands immediately
- "Imm\_Other" -- the system processes the commands as queued

## Examples

```
cluster1::> vsserver iscsi command show -instance -vsserver vs_1
      Vserver: vs_1
Target Portal Group Name: tpgroup_1
Target Session ID: 2
      Command ID: 20797
Initiator Name: ign.1993-08.org.debian:01:fa752b8a5a3a
Initiator Alias: alias_1
Initiator Session ID: 00:02:3d:01:00:00
      Command Sub ID: 20797
      Command State: Scsicdb_Waiting_STLayer
      Command Type: Sequenced
```

Displays detailed information for active iSCSI commands in Vserver vs\_1.

---

## vserver iscsi connection show

Display active iSCSI connections

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays iSCSI connection information within a session. If you do not specify a connection, the command displays all information for all connections.

An active iSCSI session can contain one or multiple iSCSI connections. If an iSCSI connection has not completed the iSCSI login sequence, the iSCSI session might not contain iSCSI connections.

This command gives real-time status of connection activity. You can use the parameters `header-digest-enabled` and `data-digest-enabled` to troubleshoot performance problems.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display iSCSI connections that match the Vserver that you specify.

[-**tpgroup** <text>] - Target Portal Group

Use this parameter to display iSCSI connections that match the target portal group that you specify.

[-**tsih** <integer>] - Target Session ID

Use this parameter to display iSCSI connections that match the target session ID that you specify.

---

**[-connection-id <integer>]** - Connection ID

Use this parameter to display iSCSI connections that match the connection ID that you specify.

**[-connection-state <iSCSI Connection State>]** - Connection State

Use this parameter to display iSCSI connections that match the connection state you specify.

**[-has-session {true|false}]** - Connection Has session

Specifies if a session is established for a connection. If you enter this command using the parameter without a value, it is set to true, and the command displays all connections that have an established session. If you set this parameter to false, the command displays all connections that do not have established sessions.

**[-lif <text>]** - Logical interface

Use this parameter to display iSCSI connections that match the logical interface that you specify.

**[-tpgroup-tag <integer>]** - Target Portal Group Tag

Use this parameter to display iSCSI connections that use the target portal group tag that you specify.

**[-local-address <text>]** - Local IP Address

Use this parameter to display iSCSI connections that use the local IP address that you specify.

**[-local-ip-port <integer>]** - Local TCP Port

Use this parameter to display iSCSI connections that use the local TCP port that you specify.

**[-authentication-method {CHAP|deny|none}]** - Authentication Type

Use this parameter to display iSCSI connections that match the authentication type that you specify. CHAP requires password validation. Deny does not allow connections. None allows all connections.

**[-data-digest-enabled {true|false}]** - Data Digest Enabled

Specifies if data digest is enabled for a connection. If you enter this command using the parameter without a value, it is set to true, and the command displays all connections that support data digest. If you set this parameter to false, the command displays all connections that do not support data digest.

**[-header-digest-enabled {true|false}]** - Header Digest Enabled

---

Specifies if header digest is supported. If you enter this command using the parameter without a value, it is set to true, and the command shows all connections that support header digest. If you set this parameter to false, the command displays all connections that do not support header digest.

**[-rcv-window-size <integer>]** - TCP/IP Recv Size

Use this parameter to display iSCSI connections that match the specified negotiated size of the TCP/IP receive window in bytes.

**[-initiator-mrdsi <integer>]** - Initiator Max Recv Data Length

Use this parameter to display iSCSI connections that match the maximum length of message that the initiator can receive.

**[-remote-address <text>]** - Remote IP address

Use the parameter to display iSCSI connections that match the IP address of the initiator that you specify.

**[-remote-ip-port <integer>]** - Remote TCP Port

Use this parameter to display iSCSI connections that match the specified TCP port of initiator that you specify.

**[-target-mrdsi <integer>]** - Target Max Recv Data Length

Use this parameter to display iSCSI connections that match the maximum message size that a target can receive.

## Examples

```
cluster1::>vserver iscsi connection show -vserver vs_1
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         TSID         ID    Address    Address     Size
-----
vs_1         vs_1.iscsi   6     0 10.63.8.163 10.60.141.65 131400
vs_1         vs_1.iscsi   7     0 10.63.8.163 10.62.8.75   131400
2 entries were displayed.
```

Displays connection information on Vserver vs\_1.

---

## vserver iscsi connection shutdown

Shut down a connection on a node

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command shuts down a specified iSCSI connection within a session. If you want to shut down all iSCSI connections in a session, use the `vserver iscsi session shutdown` command.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-tpgroup** <text> - Target Portal Group

Specifies the target portal group that contains the connection you want to shut down.

**-tsih** <integer> - Target Session ID

Specifies the target session ID that you want to shut down.

**-connection-id** <integer> - Connection ID

Specifies the connection ID that you want to shut down.

### Examples

```
cluster1::*> vserver iscsi connection shutdown -vserver vs_1 -tpgroup tpgroup_1 -tsih 4 -connection-id 0
```

Forces the shutdown of an iSCSI connection with the connection ID of 0 on Vserver `vs_1` in tpgroup `tpgroup_1`, target session ID 4.

### See Also

`vserver iscsi session shutdown`

---

## vserver iscsi initiator show

Display iSCSI initiators currently connected

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays a list of active initiators currently connected to a specified Vserver.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display the active initiators that match the Vserver that you specify.

[-**tpgroup** <text>] - Target Portal Group

Use this parameter to display the active initiators that match the name of the target portal group that you specify.

[-**tsih** <integer>] - Target Session ID

Use this parameter to display the active initiators that match the target session ID you that specify.

[-**initiator-name** <text>] - Initiator Name

Use this parameter to display the active initiators that match the initiator name that you specify.

[-**initiator-alias** <text>] - Initiator Alias

---

Use this parameter to display the active initiators that match the alias name that you specify.

**[-tpgroup-tag <integer>]** - TPGGroup Tag

Use this parameter to display the active initiators that match the target portal group tag that you specify.

**[-isid <text>]** - Initiator Session ID

Use this parameter to display the active initiators that match the initiator session ID that you specify.

**[-igroup <text>, ...]** - Igroup Name

Use this parameter to display the active initiators that match the initiator group that you specify.

### Examples

```
cluster1::> vserver iscsi initiator show -vserver vs_1
Vserver  Tpgroup  Initiator
Name     Name      Name      ISID      IGroup
-----
vs_1     vs_1.iscsi  6  iqn.1994-05.com.redhat:6ed6dfb0489e
vs_1     vs_1.iscsi  7  iqn.1993-08.org.debian:01:fa752b8a5a3a
2 entries were displayed.
```

Displays the active initiator information on Vserver vs\_1.



---

## vserver iscsi interface disable

Disable the specified interfaces for iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command disables the specified logical interfaces for an iSCSI service. Once disabled, all subsequent attempts to establish new iSCSI connections over the logical interface will fail.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

{ **-lif** <lif-name>, ... - Logical Interface

Specifies the logical interfaces on a Vserver you want to disable.

| **-all** | **-a** [true] } - All

Specifies that all logical interfaces on the Vserver are disabled.

[**-force** | **-f** [true]] - Force

When set to true, forces the termination of any active iSCSI sessions without prompting you for a confirmation.

### Examples

```
cluster::> vserver iscsi interface disable -vserver vs_1 -lif vs_1.iscsi
```

Disables the iscsi logical interface vs\_1.iscsi on Vserver vs\_1.

---

## vserver iscsi interface enable

Enable the specified interfaces for iSCSI service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command enables specified logical interfaces for iSCSI Vserver service. Once enabled, your system accepts new iSCSI connections and services iSCSI requests over the newly enabled logical interfaces.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

{ **-lif** <lif-name>, ... - Logical Interface

Specifies the logical interfaces on a Vserver that you want to enable.

| **-all** | **-a** [true] } - All

When set to true, all logical interfaces are enabled. If you use this parameter without a value, it is set to true, and the command enables all logical interfaces.

### Examples

```
cluster1::> vserver iscsi interface enable -vserver vs_1 -lif vs_1.iscsi
```

Enables the iscsi logical interface vs\_1.iscsi on Vserver vs\_1.

---

## vserver iscsi interface show

Show network interfaces used for iSCSI connectivity

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command shows the iSCSI logical interfaces for a specified Vserver. If you do not specify any of the parameters, the command displays all of the interfaces on a Vserver.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display iSCSI logical interfaces that match the Vserver that you specify.

[-**lif** <lif-name>] - Logical Interface

Use this parameter to display iSCSI logical interfaces that that you specify.

[-**status-admin** {up|down}] - Administrative Status

Specifies the configured status of the logical interface. If you set this parameter to up, the command displays all iSCSI logical interfaces with the administrative status of up. If you set this parameter to down, the command displays all the iSCSI logical interfaces with the administrative status of down.

[-**status-oper** {up|down}] - Operational Status

Specifies the current status of the logical interface. If you set this parameter to up, the command displays all the iSCSI logical interfaces with the operational status of up. If you set this parameter to down, the command displays all the iSCSI logical interfaces with the operational status of down.

---

**[-enabled {true|false}]** - Enabled

Specifies if this logical unit is enabled for iSCSI service. If you enter this command without a parameter, its effective value is true, and the command displays all the enabled iSCSI logical interfaces.

**[-address <IP Address>]** - IP Address

Use this parameter to display iSCSI logical interfaces that match the IP address that you specify.

**[-ip-port <integer>]** - IP Port Number

Use this parameter to display iSCSI logical interfaces that match IP port number for the logical interface that you specify.

**[-curr-node <nodename>]** - Current Node

Use this parameter to display iSCSI logical interfaces that match current node that you specify.

**[-curr-port {<netport>|<ifgrp>}]** - Current Port

Use this parameter to display iSCSI logical interfaces that match specified current physical port that you specify.

**[-is-home {true|false}]** - Is Home

Specifies if the node hosting the logical interface is the initially configured node. If you use this command without using this parameter, it is set to true, and the command displays all iSCSI interfaces that are on the initially configured node.

**[-tpgroup <text>]** - TPGGroup Name

Use this parameter to display iSCSI logical interfaces that match the target portal group name that you specify.

**[-tpgroup-tag | -t <integer>]** - TPGGroup Tag

Use this parameter to display iSCSI logical interfaces that match the target portal group tag that you specify.

**[-relative-port-id <integer>]** - Relative Port ID

Use this parameter to display iSCSI logical interface that matches the relative target port ID that you specify. The system assigns each logical interfaces and target portal group a relative target port ID that is Vserver unique. You cannot change this ID.

## Examples

```
cluster1::> vserver iscsi interface show -vserver vs_1
              Logical      Status      IP      Curr      Curr
```

---

Vserver	Interface	TPGT	Admin/Oper	Address	Node	Port	Enabled
vs_1	vs_1.iscsi	1027	up/up	10.63.8.165	node1	e0c	true
vs_1	vs_1.iscsi2	1028	up/up	10.63.8.166	node1	e0c	true

2 entries were displayed.

Displays information for logical interfaces on Vserver vs\_1.

```
cluster1::> vserver iscsi interface show -vserver vs_1 -relative-port-id 1
```

Vserver	Logical Interface	TPGT	Status Admin/Oper	IP Address	Curr Node	Curr Port	Enabled
vs_1	vs_1.iscsi	1027	up/up	10.63.8.165	node1	e0c	true

Displays the logical interface vs\_1.iscsi with the relative target port ID of 1.

---

## vserver iscsi interface accesslist add

Add the iSCSI LIFs to the accesslist of the specified initiator

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command adds network interfaces to an access list for a specified initiator. An access list ensures that an initiator only logs in with IP addresses associated with the interfaces defined in the access list.

You can restrict an initiator to certain network interfaces to improve performance and security. Access lists are useful where a particular initiator cannot access all of the network interfaces on a node.

Access list policies are based on the interface name. The accesslist rules are:

- If you disable the network interface for iSCSI through the `vserver iscsi interface disable` command, for example, the network interface is not accessible to any initiator regardless of any access lists in effect.
- If an initiator does not have an access list, that initiator can access any iSCSI-enabled network interface.
- If an initiator has an access list, that initiator can only login to network interfaces in its access list. Additionally, the initiator cannot discover any IP addresses that are not on this access list. If an initiator sends an iSCSI `sendtargets` request, the node responds with a list of IP addresses for iSCSI data logical interfaces that are in its access list.
- If an initiator does not have an access list, you automatically create an access list when you issue the `vserver iscsi interface accesslist add` command.
- If you remove all the interfaces from the access list of an initiator with the `vserver iscsi interface accesslist remove` command, the accesslist is also deleted.
- Creating or modifying access list requires that initiator log out and log back in before changes take effect.

When you use the add or remove commands, the system warns you if an iSCSI session could be affected.

---

Note:

You will not affect any iSCSI sessions if you use the `-a` parameter when adding or removing all interfaces.

## Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver name.

**-initiator-name** <text> - Initiator Name

Specifies the initiator you want to add to the access list.

{ **-lif** <lif-name>, ... - Logical Interface

Specifies the lif you want to add to an access list.

| **-all** | **-a** [true] } - All

If you use this parameter without a value, it is set to true, and the command adds all iSCSI data logical interfaces for a vserver to an initiator's accesslist. If the initiator does not have an accesslist, the system creates a new accesslist.

[**-force** | **-f** [true]] - Force

If you use this parameter without a value, it is set to true, and the command does not prompt you when an active iSCSI service or any active iSCSI data logical interfaces could be affected. If you do not use this parameter, the command prompts for confirmation if the iSCSI service is active or if any active data logical interfaces would be affected.

## Examples

```
cluster1::>vserver iscsi interface accesslist add -vserver vs_1 -initiator-name  
iqn.1992-08.com.example:abcdefg -a
```

Adds the initiator `iqn.1992-08.com.example:abcdefg` on Vserver `vs_1` for all iSCSI data logical interfaces in `vs_1`.

## See Also

`vserver iscsi interface disable`   `vserver iscsi interface accesslist remove`

---

## vserver iscsi interface accesslist remove

Remove the iSCSI LIFs from the accesslist of the specified initiator

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command removes network interfaces from an access list for a specified initiator. The system removes the access list when the list is empty. When you remove a network interface from an initiator, this action could result in the shutdown of active sessions.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver name.

**-initiator-name** <text> - Initiator Name

Specifies the initiator that you want to remove logical interfaces from.

{ **-lif** <lif-name>, ... - Logical Interface

Specifies the logical interface you want to remove.

| **-all** | **-a** [true] } - All

If you use this parameter without a value, it is set to true, and the command removes all of the iSCSI data logical interfaces from an initiator's accesslist. If you remove all the network interfaces from an access list, the system removes the access list.

[**-force** | **-f** [true]] - Force

If you use this parameter without a value, it is set to true, and the command does not prompt you when an active iSCSI service or any active iSCSI data logical interfaces could be affected. If you do not use this parameter, the command prompts for confirmation if the iSCSI service is active or if any active data logical interfaces would be affected.

### Examples

```
cluster1::> vserver iscsi interface accesslist remove -vserver vs_1 -initiator-  
name iqn.1992-08.com.example:abcdefg -a
```



---

Removes all the network interfaces from the access list for initiator  
iqn.1992-08.com.example:abcdefg on Vserver vs\_1.

---

## vserver iscsi interface accesslist show

Show accesslist of the initiators for iSCSI connectivity

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays an access list for an initiator. An access list is a list of logical interfaces that an initiator can use for iSCSI logins. The system records the access lists as part of the node configuration and preserves the access lists during reboots.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

Use this parameter to display the access lists that match the Vserver name that you specify.

**[-initiator-name <text>]** - Initiator Name

Use this parameter to display the access lists that match the initiator that you specify.

**[-lif <lif-name>]** - Logical Interface

Use this parameter to display the access lists that match the logical interface that you specify.

### Examples

```
cluster1::> vserver iscsi interface accesslist show -vserver vs_1
Vserver      Initiator Name      Logical Interface
-----
vs1          iqn.2010-01.com.example:aaaaa  isw1
                                     isw2
                                     iqn.2010-01.com.example:aaabb  isw1
                                     isw2
4 entries were displayed.
```

---

Displays the access lists for vserver vs\_1

---

## vserver iscsi isns create

Configure the iSNS service for the Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command creates an iSNS service with the IP address of the iSNS server. You should configure the iSNS service before the iSNS service is started.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to create.

**-address** <IP Address> - iSNS Server IP Address

Specifies the IP address of the iSNS server. Both IPv4 and IPv6 address families are supported. The address family must be the same as that of the vservers management LIF.

Note:

A default route must exist for the specified vservers. To create a route, use the `network routing-groups route create` command. To view existing routes, use the `network routing-groups route show` command.

**[-status-admin {down|up}]** - Administrative Status

Specifies the administrative status of the iSNS service of a Vserver. If you set this parameter to up, the iSNS service starts for the Vserver and registers with the configured iSNS server. If you set this parameter to down, the Vserver loses its ability to register with the iSNS server and to be discovered by iSNS clients.

**[-force [true]]** - Force

`vserver iscsi isns create` fails if vservers management LIF is not configured. When you set this option to "true," you create an iSNS service on a Vserver even if the vservers does not have a vservers management LIF.

### Examples

---

```
cluster::> vserver iscsi isns create -vserver vs_1 -address 10.60.1.1 -status-admin up
```

Creates the iSNS service for Vserver vs\_1 using the IPv4 address.

```
cluster::> vserver iscsi isns create -vserver vs_1 -address fd20:8b1e:b255:840b:a0df:565b:19b5:4d06 -status-admin up
```

Creates the iSNS service for Vserver vs\_1 using the IPv6 address.

## See Also

[network routing-groups route create](#)   [network routing-groups route show](#)

---

## vserver iscsi isns delete

Remove the iSNS service for the Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command deletes the iSNS service for the Vserver.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to delete.

### Examples

```
cluster::> vserver iscsi isns delete -vserver vs_1
```

Deletes the iSNS service for Vserver vs\_1.

---

## vserver iscsi isns disable

Disable isns capability

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command disables the iSNS capability for the cluster. This action disables the iSNS service on all iSNS configured Vservers present in the cluster.

Note:

This does not block subsequent attempts to create or modify iSNS services.

### Parameters

None

### Examples

```
cluster::*> set advanced
Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

```
cluster::*> iscsi isns show
Vserver      iSNS Server Entity Identifier  iSNS Server IP Address  iSNS Status
-----
vs1          isns:00000101                 172.219.236.188         up
vs2          isns:00000054                 172.219.236.198         up
2 entries were displayed.
```

```
cluster::*> iscsi isns disable
```

```
cluster::*> iscsi isns show
Vserver      iSNS Server Entity Identifier  iSNS Server IP Address  iSNS Status
-----
vs1          isns:00000101                 172.219.236.188         down
vs2          isns:00000054                 172.219.236.198         down
2 entries were displayed.
```

Disables iSNS capability of the cluster. iSNS service is also disabled for all iSNS configured Vservers present in the cluster.

---

## vserver iscsi isns modify

Modify the iSNS service for the Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command modifies the configuration of an iSNS service.

Modifications take effect immediately after you execute the command.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to modify.

**[-address** <IP Address>] - iSNS Server IP Address

Specifies the IP address of the iSNS server. Both IPv4 and IPv6 address families are supported. The address family must be the same as that of the vservers management LIF.

Note:

A default route must exist for the specified vservers. To create a route, use the `network routing-groups route create` command. To view existing routes, use the `network routing-groups route show` command.

**[-status-admin** {down|up}] - Administrative Status

Specifies the administrative status of the iSNS service of a Vserver. If you set this parameter to up, the iSNS service starts for the Vserver, and registers with the configured iSNS server. If you set this parameter to down, the Vserver loses its ability to register with the iSNS server and to be discovered by iSNS clients.

**[-force** [true]] - Force

`vserver iscsi isns modify` fails to modify the iSNS server address if vservers management LIF is not configured. When you set this option to "true," you can modify the iSNS service on a Vserver even if the vservers does not have a vservers management LIF.



---

## Examples

```
cluster::> iscsi isns modify -vserver vs_1 -status-admin up
```

Modifies the status-admin of the iSNS service for Vserver vs\_1 to up.

## See Also

network routing-groups route create   network routing-groups route show

---

## vserver iscsi isns show

Show iSNS service configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Shows the iSNS service configuration.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver Name

Use this parameter to display the iSNS services that match the Vserver name that you specify.

[-**address** <IP Address>] - iSNS Server IP Address

Use this parameter to display the iSNS services that match the IP address of the iSNS server that you specify.

[-**status-admin** {down|up}] - Administrative Status

Use this parameter to display the iSNS services that match the configured status of the service that you specify.

[-**entity-id** <text>] - iSNS Server Entity Id

Use this parameter to display the iSNS services that match the configured iSNS server entity-id that you specify.

[-**last-successful-update** <MM/DD/YYYY HH:MM:SS>] - Last Successful Update

Use this parameter to display the iSNS services that match the time of the last successful attempt.

---

**[`-last-update-attempt` <MM/DD/YYYY HH:MM:SS>]** - Last Update Attempt

Use this parameter to display the iSNS services that match the time of the last update attempt.

**[`-last-update-result` <isnsErrors>]** - Last Update Result

Use this parameter to display the iSNS services that match the result of the last update attempt.

## Examples

```
cluster::> vserver iscsi isns show
Vserver      iSNS Server Entity Identifier  iSNS Server IP Address  iSNS Status
-----
iscsi_vs     isns:00000044                  10.229.136.188          up
```

Displays the output of the show command for all Vservers in a cluster.

```
cluster::> vserver iscsi isns show -instance
      Vserver Name: vs1
iSNS Server IP Address: 10.72.19.11
Administrative Status: up
iSNS Server Entity Id: isns.0000001c
Last Successful Update: 11/12/2011 10:18:45
Last Update Attempt: 11/12/2011 10:18:45
Last Update Result: iSNS_Ok
```

```
      Vserver Name: vs2
iSNS Server IP Address: 10.72.16.13
Administrative Status: up
iSNS Server Entity Id: isns.0000001b
Last Successful Update: 11/12/2011 13:38:05
Last Update Attempt: 11/12/2011 13:38:05
Last Update Result: iSNS_Ok
```

2 entries were displayed.

Displays the details for all Vservers in a cluster.

---

## vserver iscsi isns start

Starts the iSNS service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Starts the iSNS service. Once you start the iSNS service, the Vserver automatically register with the iSNS server.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to start.

### Examples

```
cluster::> vserver iscsi isns start -vserver vs_1
```

Starts the iSNS service for Vserver vs\_1.

---

## vserver iscsi isns stop

Stops the iSNS service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Stops the iSNS service. Once you stop the iSNS service, the Vserver loses the ability to register with the iSNS server and to be discovered by iSNS clients.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to stop.

### Examples

```
cluster::> vserver iscsi isns stop -vserver vs_1
```

Stops the iSNS service for Vserver vs\_1.

---

## vserver iscsi isns update

Force update of registered iSNS information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Forces an update of the registration information with the iSNS server. Normally, the system checks for iSNS configuration changes on the Vserver every few minutes and automatically sends updates to the iSNS server.

### Parameters

**-vserver** <vserver name> - Vserver Name

Specifies the Vserver for the iSNS service that you want to update.

### Examples

```
cluster::> vserver iscsi isns update -vserver vs_1
```

Updates the iSNS server registration for Vserver vs\_1.

---

## vserver iscsi security create

Create an iSCSI authentication configuration for an initiator

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command configures the security method for an iSCSI initiator on a Vserver. The outbound CHAP password and user name are optional. If you want mutual authentication, you need to configure both inbound and outbound CHAP passwords and user names.

You cannot use the same password for inbound and outbound settings.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-initiator-name** | **-i** <text> - Initiator Name

Specifies the initiator that you want to create a security method for. You can use either an iqn such as iqn.2010-12.com.example:ABCDEFGH or eui such as eui.5000ABCD78945E21 for the initiator.

**-auth-type** | **-s** {CHAP|deny|none} - Authentication Type

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.
- deny - The initiator cannot access the Vserver.

**[-user-name | -n <text>]** - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

**[-outbound-user-name | -m <text>]** - Outbound CHAP User Name

---

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

## Examples

```
cluster1::> iscsi security create -initiator eui.10123456789ABCDE -auth-type CHAP  
-user-name bob -outbound-user-name bob2
```

```
    Password:
```

```
    Outbound Password:
```

Creates authentication method chap for initiator eui.10123456789ABCDE with inbound and outbound usernames and passwords.



---

## vserver iscsi security default

Configure the default authentication settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command defines a default iSCSI authentication method for your Vserver. If you do not configure the initiator to use a user-defined authentication method, the system assigns the default authentication method automatically to the initiator. Use the `vserver iscsi security create` command if you want to configure a user-defined authentication method.

The outbound CHAP user name and password are optional. If you want a bi-directional handshake, provide the outbound user name and you will be prompted for the corresponding password.

You cannot use the same password for inbound and outbound settings.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-auth-type** | **-s** {CHAP|deny|none} - Authentication Method

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.
- deny - The initiator cannot access the Vserver.

**[-user-name | -n <text>]** - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

**{ [-outbound-user-name | -m <text>]** - Outbound CHAP User Name

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

---

| **[-clear-outbound [true]] }** - Clear Outbound CHAP Parameters

Removes the outbound user name and the outbound password information from the default authentication method. After you clear the outbound information, you no longer have a bi-directional handshake.

## Examples

```
cluster1::> iscsi security default -vserver vs_1 -security chap -user-name bob -  
outbound-user-name bob_out
```

Password:

Outbound Password:

Sets the default authentication method to CHAP with inbound and outbound user names and passwords.

## See Also

vserver iscsi security create

---

## vserver iscsi security delete

Delete the iSCSI authentication configuration for an initiator

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command removes the security settings for this initiator. The default authentication setting now applies to this initiator.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-initiator-name** | **-i** <text> - Initiator Name

Specifies the initiator that you want to remove the authentication setting from.

### Examples

```
cluster1::> iscsi security delete -vserver vs_1 -initiator  
iqn.1992-08.com.example:abcdefg
```

Deletes initiator iqn.1992-08.com.example:abcdefg on Vserver vs\_1 from the authentication setting. The default authentication now applies to this initiator.

---

## vserver iscsi security generate

Generate a 128-bit random CHAP secret

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command generates a 128-bit value that you can use as a CHAP secret.

### Parameters

None

### Examples

```
cluster1::> vserver iscsi security generate  
Generated Random Secret: 0x1c755035c7a64c302d4fa2459223f205
```

Generates a random secret password.

---

## vserver iscsi security modify

Modify the iSCSI authentication configuration for an initiator

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The command modifies an existing authentication method for an initiator. To delete the authentication setting for an initiator, use the `vserver iscsi security delete` command.

The outbound CHAP password and user name are optional. If you want a bi-directional handshake, you need to configure both inbound and outbound CHAP passwords and user names.

You do not need to know the inbound or outbound passwords to change them.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-initiator-name** | **-i** <text> - Initiator Name

Specifies the initiator name that you want to modify the existing authentication method.

**[-auth-type | -s** {CHAP|deny|none}] - Authentication Type

Specifies the authentication type:

- CHAP - Authenticates using a CHAP user name and password.
- none - The initiator can access the Vserver without authentication.
- deny - The initiator cannot access the Vserver.

**[-user-name | -n** <text>] - Inbound CHAP User Name

Specifies the inbound CHAP user name. CHAP user names can be one to 128 bytes. A null user name is not allowed. If provided, you will be prompted to provide the corresponding inbound CHAP password.

{ **[-outbound-user-name | -m** <text>] - Outbound CHAP User Name

---

Specifies the outbound CHAP user name. CHAP user names can be one to 128 bytes. If provided, you will be prompted to enter the corresponding outbound CHAP password.

| **[-clear-outbound [true]]** } - Clear Outbound CHAP Parameters

Removes the outbound user name and the outbound password information from the authentication method. After you clear the outbound information, you no longer have a bi-directional handshake.

## Examples

```
cluster1::> vserver iscsi security modify -vserver vs_1 -initiator
iqn.1992-08.com.example:abcdefg -auth-type chap -user-name bob -outbound-user-
name bob_out
```

Password:

Outbound Password:

Changes user names and passwords for initiator iqn.1992-08.com.example:abcdefg on Vserver vs\_1.

## See Also

vserver iscsi security delete

---

## vserver iscsi security show

Show the current iSCSI authentication configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays the default authentication and all initiator-specific authentication information. Data ONTAP authentication overrides all other service authentication methods.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

Use this command to display authentication information that matches the Vserver name that you specify.

**[-initiator-name | -i <text>]** - Initiator Name

Use this command to display authentication information that matches the initiator that you specify.

**[-auth-type | -s {CHAP|deny|none}]** - Authentication Type

Use this command to display authentication information that matches the authentication type that you specify.

**[-user-name | -n <text>]** - Inbound CHAP User Name

Use this command to display authentication information that matches the inbound CHAP user name that you specify.

**[-outbound-user-name | -m <text>]** - Outbound CHAP User Name

---

Use this command to display authentication information that matches the outbound CHAP user name that you specify.

**[-auth-chap-policy <local>] - Authentication CHAP Policy**

Use this command to display authentication information that matches the authentication CHAP policy that you specify.

**Examples**

```
cluster1::> iscsi security show -vserver vs_1
Vserver      Initiator Name      Auth      Auth CHAP  Inbound CHAP  Outbound CHAP
-----      -
vs_1         default             none      -           -             -
vs_1         iqn.2010-12.com.example:abcdefg
CHAP         local              bob       bob2
2 entries were displayed.
```

Displays the authentication information for Vserver vs\_1.



---

## vserver iscsi session show

Display iSCSI sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays iSCSI session information. If you do not specify the target session ID (TSIH), the command displays all session information for the specified Vserver. If a Vserver is not specified, the command displays all session information in the cluster. Use the `vserver iscsi connection show` command to display connection information. Use the `vserver iscsi session parameter show` command to show the parameters used when creating the session.

You can use session information for troubleshooting performance problems.

An iSCSI session can have one or multiple connections. Typically a session has at least one connection.

Most of the parameters are read-only. However, some parameters can be modified with the `vserver iscsi modify` command.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Use this parameter to display iSCSI session information that matches the Vserver name that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display iSCSI session information that matches the target portal group name that you specify.

---

**[-tsih <integer>]** - Target Session ID

Use this parameter to display iSCSI session information that matches the target session ID that you specify.

**[-max-ios-per-session <integer>]** - Max Commands per Session

Use this parameter to display iSCSI session information that matches the maximum commands per session count you specify.

**[-data-pdu-in-order {true|false}]** - Data PDU in Order

Specifies if the data PDUs are in sequence order. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports PDUs in order. If you provide a false value, the command displays all session information that does not support PDUs in order.

**[-data-sequence-in-order {true|false}]** - Data Sequence in Order

Specifies if the data is in sequence order. If you enter this command without using this parameter, it is set to true, and the command displays all session information where data sequence is supported. If you provide a false value, the command displays all session information that does not support data sequence.

**[-default-time-to-retain <integer>]** - Default Time to Retain

Use this parameter to display session information that matches the retain time that you specify. This value specifies the amount of time before active reassignment is possible after an unexpected connection termination or a connection reset. A value of 0 means the connection task state is immediately discarded by the target.

**[-default-time-to-wait <integer>]** - Default Time to Wait

Use this parameter to display session information that matches the logout or active task assignment wait time that you specify. Wait time refers to the amount of time before attempting an explicit or implicit logout or active task assignment after an unexpected connection termination or connection reset.

**[-error-recovery-level <integer>]** - Error Recovery Level

Use this command to display session information that matches the error recovery level that you specify.

**[-first-burst-length <integer>]** - First Burst Length

Use this parameter to display session information that matches the first burst length that you specify. First burst length is the maximum amount of unsolicited data in bytes that can be sent during the execution of a single iSCSI packet. First burst length covers the total amount of immediate data and the unsolicited data-out PDU. The first burst length must not exceed the maximum burst length.

---

**[-immediate-data-enabled {true|false}]** - Immediate Data

Specifies if immediate data is supported. When immediate data is supported, the initiator can send immediate data. If you enter this command using the parameter without a value, it is set to true, and the command displays all session information that supports immediate data. If you provide a false value, the command displays all session information that does not support immediate data.

**[-initiator-alias <text>]** - Initiator Alias

Use this parameter to display iSCSI session information that matches the alias name of the initiator that you specify.

**[-initial-r2t-enabled {true|false}]** - Initial R2T Enabled

Specifies if the initiator supports Initial Ready to Transfer (R2T). R2T is the mechanism that allows the target to request the initiator for output data. If you enter this command using the parameter without a value, it is set to true, and the command displays all session information that supports initial R2T data. If you provide a false value, the command displays all session information that does not support initial R2T data.

**[-initiator-name <text>]** - Initiator Name

Use this parameter to display the iSCSI session information that matches the initiator name that you specify.

**[-isid <text>]** - Initiator Session ID

Use this parameter to display iSCSI session information that matches the initiator session ID that you specify.

**[-max-burst-length <integer>]** - Max Burst Length for Session

Use this parameter to display iSCSI session information that matches the maximum burst length that you specify. Maximum burst length is the maximum iSCSI data payload in bytes for a data-in or solicited data-out sequence.

**[-max-connections <integer>]** - Max Connections for Session

Use this parameter to display iSCSI session information that matches the maximum number of connections that you specify.

**[-max-outstanding-r2t <integer>]** - Max Outstanding R2T for Session

Use this parameter to display iSCSI session information that matches the maximum number of outstanding R2T per task that you specify.

**[-session-type <iSCSI Session Type>]** - Session Type

Use this parameter to display iSCSI session information that matches the session type that you specify.

---

**[-tpgroup-tag <integer>]** - Target Portal Group Tag

Use this parameter to display iSCSI session information that matches the target portal group tag that you specify.

**[-connection-ids <integer>, ...]** - Active Connection IDs

Use this parameter to display iSCSI session information that matches the active connection IDs that you specify.

**Examples**

```
cluster::> vserver iscsi session show -vserver vs_1
Vserver  Tpgroup  TSIH  Initiator  ISID  Initiator
Name     Name     Name                                     Alias
-----  -----  ----  -
vs_1     tpgroup_1  2      iqn.1993-08.org.debian:01:fa752b8a5a3a
                                           00:02:3d:01:00:00
                                           initiator-alias
Displays session information for all sessions on Vserver vs_1.
```

**See Also**

vserver iscsi connection show   vserver iscsi session parameter show  
vserver iscsi modify

---

## vserver iscsi session shutdown

Shut down a session on a node

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command forces a shutdown of all connections in a session. If you want to shut down a single connection in a session, use the `vserver iscsi connection shutdown` command.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver.

**-tpgroup** <text> - Target Portal Group

Specifies the target portal group that contains the session you want to shutdown.

**-tsih** <integer> - Target Session ID

Specifies the target session ID that you want to shut down.

### Examples

```
cluster::*> vserver iscsi session shutdown -vserver vs_1 -tpgroup tpgroup_1 -tsih 2
```

Forces a session shutdown for target session ID 2 in tpgroup\_1 in Vserver vs\_1 .

### See Also

`vserver iscsi connection shutdown`

---

## vserver iscsi session parameter show

Display the parameters used to establish an iSCSI session

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command displays session parameter information. This command is intended for troubleshooting performance problems.

Most of the parameters are read-only. However, some parameters can be modified with the `vserver iscsi modify` command.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Use this parameter to display session information that matches the Vserver name that you specify.

[-tpgroup <text>] - Target Portal Group

Use this parameter to display session information that matches the target portal group name that you specify.

[-tsih <integer>] - Target Session ID

Use this parameter to display session information that matches the target session ID that you specify.

[-cmd-window-size <integer>] - Max Commands per Session

Use this parameter to display session information that matches the command window size that you specify.

---

**[-data-pdu-in-order {true|false}]** - Data PDU in Order

Use this parameter to display session information with the value of the Protocol Data Units (PDU) in order flag you specify. This parameter indicates if the data within a sequence can be in any order or must be in sequence. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports PDUs in order. If you provide a false value, the command displays all session information that does not support PDUs in order.

**[-data-sequence-in-order {true|false}]** - Data Sequence in Order

Use this parameter to display session information with the value of the data sequence in order flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports data sequence. If you set the values to false, the command displays all session information that does not support data sequence.

**[-default-time-to-retain <integer>]** - Default Time to Retain

Use this parameter to display session information that matches the retain time that you specify. This value specifies the amount of time before active reassignment is possible after an unexpected connection termination or a connection reset. A value of 0 means the connection task state is immediately discarded by the target.

**[-default-time-to-wait <integer>]** - Default Time to Wait

Use this parameter to display session information that matches the logout or active task assignment wait time that you specify. Wait time refers to the amount of time before attempting an explicit or implicit logout or active task assignment after an unexpected connection termination or connection reset.

**[-error-recovery-level <integer>]** - Error Recovery Level

Use this command to display session information that matches the error recovery level that you specify.

**[-first-burst-length <integer>]** - First Burst Length

Use this parameter to display session information that matches the first burst length that you specify. First burst length is the maximum amount of unsolicited data in bytes that can be sent during the execution of a single iSCSI packet. First burst length covers the total amount of immediate data and the unsolicited data-out PDU. The first burst length must not exceed the maximum burst length.

**[-immediate-data-enabled {true|false}]** - Immediate Data

Use this parameter to display session information with the value of the immediate data-enabled flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports immediate

---

data. If you set the value to false, the command displays all session information that does not support immediate data.

**[-initial-r2t-enabled {true|false}]** - Initial R2T Enabled

Use this parameter to display session information with the value of the R2T data-enabled flag that you specify. If you enter this command without using this parameter, it is set to true, and the command displays all session information that supports R2T data. If you set the value to false, the command displays all session information that does not support R2T data.

**[-initiator-alias <text>]** - Initiator Alias

Use this parameter to display iSCSI session information that matches the initiator alias name you specify.

**[-initiator-name <text>]** - Initiator Name

Use this parameter to display iSCSI session information that matches the initiator name you specify.

**[-isid <text>]** - Initiator Session ID

Use this parameter to display iSCSI session information that matches the initiator session identifier you specify.

**[-max-burst-length <integer>]** - Max Burst Length for Session

Use this parameter to display iSCSI session information that matches the maximum burst length that you specify. Maximum burst length is the maximum iSCSI data payload in bytes for a data-in or solicited data-out sequence.

**[-max-connections <integer>]** - Max Connections for Session

Use this parameter to display iSCSI session information that matches the maximum number of connections that you specify.

**[-max-outstanding-r2t <integer>]** - Max Outstanding R2T for Session

Use this parameter to display iSCSI session information that matches the maximum number of outstanding R2T per task that you specify.

**[-session-type <iSCSI Session Type>]** - Session Type

Use this parameter to display iSCSI session information that matches the session type you specify.

**[-tpgroup-tag <integer>]** - Target Portal Group Tag

Use this parameter to display iSCSI session information that matches the target portal group tag you specify.



**[-initiator-mrdsi <integer>, ...]** - Initiator Max Recv Data Len

Use this parameter to display iSCSI session information that matches the initiator maximum receivable data segment length you specify. An iSCSI initiator declares the maximum data segment length in bytes it can receive in an iSCSI PDU during the iSCSI login phase.

**[-target-mrdsi <integer>, ...]** - Target Max Recv Data Len

Use this parameter to display iSCSI session information that matches the target maximum receivable data segment length you specify. An iSCSI target declares the maximum data segment length in bytes it can receive in an iSCSI PDU during the iSCSI login phase.

**Examples**

```
cluster1:>> iscsi session parameter show -vserver vs_1
Vserver  Tpgroup      Max Data PDU Data Seq Time 2 Time 2 Error Imm Initial
Name     TSIH Conn  In Order In Order Retain Wait  Rec Lvl Data  R2T
-----
vs_1     vs_1.iscsi 6      1 true    true    0      2      0 true  false
vs_1     vs_1.iscsi 7      1 true    true    0      2      0 true  false
2 entries were displayed.
```

Lists iSCSI session parameters for Vserver vs\_1.

**See Also**

vserver iscsi modify

---

## vserver locks break

Break file locks based on a set of criteria

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver locks break` command breaks one or more locks.

### Parameters

{ **-vserver** <vserver name> - Vserver

This parameter specifies the Vserver containing the lock.

**-volume** <volume name> - Volume

This parameter specifies the name of the volume containing the lock.

**-lif** <lif-name> - Logical Interface

This parameter specifies the logical interface through which the lock was established.

**-path** <text> - Object Path

This parameter specifies a path to the lock.

| **-lockid** <UUID> } - Lock UUID

This parameter specifies the universally unique identifier (UUID) for the lock.

### Examples

The following example breaks the locks on all objects on the Vserver named `vs0` in the volume named `vol0`, regardless of the paths to the locked objects and the logical interface through which the locks were established.

```
cluster1::*> vserver locks break -vserver vs0 -volume vol0 -path * -lif *
WARNING: Breaking file locks can cause applications to become unsynchronized
and may lead to data corruption. If you are breaking a file lock on
a volume that is being accessed by a FlexCache you must take the
volume offline on the FlexCache to reestablish proper delegation
synchronization between the origin and the cache.
Do you want to continue? {y|n}: y
1 entry was acted on.
```

---

## vserver locks show

Display current list of locks

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver locks show` command displays information about locks. A lock is a synchronization mechanism for enforcing limits on concurrent access to files where many clients can be accessing the same file at the same time. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about locks:

- Vserver name
- Volume name
- Object path
- Logical interface name
- Lock protocol
- Lock type
- Client

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-smb-attrs ]

If you specify the `-smb-attrs` parameter, the command displays information related to SMB2 and higher.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

{ [-vserver <vserver name>] - Vserver

---

If you specify this parameter, the command displays information about locks on the specified Vserver.

**[-volume <volume name>]** - Volume

If you specify this parameter, the command displays information about locks on the specified volume.

**[-lif <lif-name>]** - Logical Interface

If you specify this parameter, the command displays information about locks established through the specified logical interface.

**[-path <text>]** - Object Path

If you specify this parameter, the command displays information about locks at the specified path name.

**| [-lockid <UUID>]** } - Lock UUID

If you specify this parameter, the command displays information about the lock with the specified universally unique identifier (UUID).

**[-protocol <lock protocol>]** - Lock Protocol

If you specify this parameter, the command displays information about locks established through the specified protocol. Some of the valid protocols are:

- cifs: SMB locks
- nlm: NFS3 locks
- nfsv4: NFS4.0 locks
- nfsv4.1: NFS4.1 locks
- crposix: CrPosix locks for CREATE and LINK
- flexcache\_deleg: FlexCache delegations

**[-type {byte-range|share-level|op-lock|delegation}]** - Lock Type

If you specify this parameter, the command displays information about locks of the specified lock type. The four types of locks are:

- Byte-range locks: Lock only a portion of a file.
- Share locks: Represent opened files.
- Opportunistic locks: Control client-side caching over SMB.
- Delegations: Control client-side caching over NFSv4.

---

**[-node <nodename>]** - Node Holding Lock State

If you specify this parameter, the command displays information about all locks on the specified node.

**[-lock-state <lock\_state>]** - Lock State

If you specify this parameter, the command displays information about the state of the lock. Some of the valid states are:

- granted: The lock is established.
- revoking: The server is currently coordinating with the client to change the state of this lock.
- revoked: The lock is undergoing revocation to be downgraded or released.
- adjusted: The lock is undergoing revocation to be replaced by a lock equal to or weaker than the current lock.
- subsumed: The lock is one of a set of locks that will replace a lock that is being revoked.
- gwaiting: The lock is waiting to be granted, because it conflicts with another lock.
- ewaiting: The lock is waiting to be granted or denied, allowing for appropriate revocation of other locks to take place.
- denied: The lock has been denied.
- timedout: The lock was waiting and has now timed out.
- gone: The lock is about to be released.
- unused: The lock is allocated but has not been processed into any state.

**[-bytelock-offset <integer>]** - Bytelock Starting Offset

If you specify this parameter, the command displays information about bytelocks with the specified offset value. This is the index in the file (in bytes) where the lock begins.

**[-bytelock-length <integer>]** - Number of Bytes Locked

If you specify this parameter, the command displays information about bytelocks with the specified length. This is the number of bytes that are locked by this particular lock.

**[-bytelock-mandatory {true|false}]** - Bytelock is Mandatory

If you specify this parameter, the command displays information only about mandatory bytelocks. A mandatory bytelock enforces the requirement of byte range locking on clients before accessing the associated range.

---

**[-bytelock-exclusive {true|false}]** - Bytelock is Exclusive

If you specify this parameter, the command displays information only about exclusive bytelocks. When an exclusive bytelock is granted, no other bytelock may be granted whose range overlaps it.

**[-bytelock-super {true|false}]** - Bytelock is Superlock

If you specify this parameter, the command displays information only about super-bytelocks. When a super-bytelock is granted, all other locks on that file are released, and no other operations will be allowed on that file. Super-bytelocks are used internally as part of the antivirus system.

**[-bytelock-soft {true|false}]** - Bytelock is Soft

If you specify this parameter, the command displays information only about softened bytelocks. An NFSv4 bytelock might become softened if the connection to the client is interrupted. Soft locks might be reclaimed if the client reconnects. However if another client requests a lock that conflicts with a soft lock, then the soft lock will be released.

**[-oplock-level {exclusive|level2|batch|null|read-batch}]** - Oplock Level

If you specify this parameter, the command displays information about locks with the specified oplock level. The oplock level determines which operations the client may cache locally. Those operations include opening, reading, writing, closing, and creating and destroying bytelocks on a file. The five valid oplock levels are:

- batch: The client may cache all operations on the file.
- exclusive: The client may cache reads and writes on the file.
- read-batch: The client may cache reads and opens on the file.
- level2: The client may cache reads on the file.
- null: The client may not cache any operations on the file.

**[-sharelock-mode <share lock mode>]** - Shared Lock Access Mode

If you specify this parameter, the command displays information about locks with the specified sharelock mode. The parameter has two components separated by a hyphen: the access mode followed by the share mode. The access mode specifies which operations the client is allowed to perform on the file. The share mode specifies which operations other clients are disallowed to perform. The two modes are a combination of one or more of these permissions:

- read
- write

- 
- delete
  - all
  - none

For example, the sharelock mode `read_write-deny_delete` allows the client to read and write the file, and disallows other clients to delete the file. A special mode is `delete-on-close`, which specifies that the server will delete the file as soon as it is closed.

**[-sharelock-soft {true|false}]** - Shared Lock is Soft

If you specify this parameter, the command displays information only about softened sharelocks. A NFSv4 sharelock can become softened when the connection to the client is interrupted. If the client reconnects, it might reclaim the sharelock. However, if another client creates a sharelock that conflicts with the softened sharelock, the softened sharelock will be released.

**[-delegation-type {read|write}]** - Delegation Type

If you specify this parameter, the command displays information only about locks with the specified delegation-type setting. The delegation type determines which operations the client may cache locally. The two valid delegation types are:

- read: The client may cache reads on the file.
- write: The client may cache reads and writes on the file.

**[-client-address <IP Address>]** - Client Address

If you specify this parameter, the command displays information only about locks from the specified client IP address.

**[-smb-open-type {none|durable|persistent}]** - SMB Open Type

If you specify this parameter, the command displays information only about locks with the specified SMB open type. Valid open types are

- durable: Durability is a feature of SMB2. A durable lock might become "disconnected" if the connection between the client and server is disrupted. A disconnected durable lock might be reconnected if the connection is reestablished.
- persistent: Persistence is a feature of SMB3. Persistent locks can become disconnected and later reconnected, like durable locks. Persistent locks are used to facilitate continuously available shares.
- none: The lock is neither durable nor persistent.

---

### **[-smb-connect-state <Lock Connect State>] - SMB Connect State**

If you specify this parameter, the command displays information only about locks with the specified SMB connection state. Some of the valid states are:

- **connected:** This is the normal state of a SMB lock when the server and client are connected.
- **disconnected:** If a lock is durable or persistent, it might become disconnected if the connection between the server and its client is interrupted. Disconnected locks may later be reconnected if the connection is reestablished.

### **[-smb-expiration-time <integer>] - SMB Expiration Time (Secs)**

If you specify this parameter, the command displays information only about locks with the specified SMB lock expiration time. When a lock is disconnected, `-smb-expiration-time` shows the time remaining until the lock expires. The server releases the lock after it expires.

### **[-smb-open-group-id <text>] - SMB Open Group ID**

If you specify this parameter, the command displays information only about locks with the specified SMB open group identifier. This is an opaque byte string provided by the client as the SMB lease key when the lock is first established.

## **Examples**

The following example displays default information about all locks:

```
cluster1::> vsserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
voll    /voll/notes.txt            node1_data1  cifs      share-level 192.168.1.5
        Sharelock Mode: read_write-deny_delete
        Oplock Level: read-batch
        /voll/notes1.txt      node1_data1  cifs      share-level 192.168.1.5
        Sharelock Mode: read_write-deny_delete
        Oplock Level: batch
        /voll                node1_data2  cifs      share-level 192.168.1.5
        Sharelock Mode: read-deny_delete
        /voll/notes.txt      node1_data2  cifs      share-level 192.168.1.5
        Sharelock Mode: read_write-deny_delete
        Oplock Level: read-batch
7 entries were displayed.
```

The following example displays the SMB related information about all locks:

```
cluster1::> vsserver locks show -smb-attrs
```



---

```

Vserver: vs0
Volume   Object Path          LIF          Protocol Lock Type  Client
-----
voll1    /voll/notes.txt            node1_data1  cifs      share-level 192.168.1.5
Sharelock Mode: read_write-deny_delete
Open Type: durable      Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d37047058909c00000000873d210700000000

                                           op-lock      192.168.1.5
Oplock Level: read-batch
Open Type: -            Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d37047058909c00000000873d210700000000

      /voll/notes1.txt            node1_data1  cifs      share-level 192.168.1.5
Sharelock Mode: read_write-deny_delete
Open Type: durable      Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d370440fc8891000000005a3f210700000000

                                           op-lock      192.168.1.5
Oplock Level: batch
Open Type: -            Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d370440fc8891000000005a3f210700000000

      /voll1                      node1_data2  cifs      share-level 192.168.1.5
Sharelock Mode: read-deny_delete
Open Type: none         Connect State: connected      Expiration Time (Secs): -
Open Group ID: -

      /voll/notes.txt            node1_data2  cifs      share-level 192.168.1.5
Sharelock Mode: read_write-deny_delete
Open Type: durable      Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d370408e08d9c00000000da40210700000000

                                           op-lock      192.168.1.5
Oplock Level: read-batch
Open Type: -            Connect State: connected      Expiration Time (Secs): -
Open Group ID: 625e2ff46ee5df1194ba0050569d370408e08d9c00000000da40210700000000
7 entries were displayed.

```

The following example displays default information about all locks in list form:

```

cluster1:> vserver locks show -instance

      Vserver: vs0
      Volume: voll
      Logical Interface: node1_data1
      Object Path: /voll/notes.txt
      Lock UUID: 447db184-f801-11df-8bb5-00a098000e34
      Lock Protocol: cifs
      Lock Type: share-level
Node Holding Lock State: node1
      Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
      Oplock Level: -
Shared Lock Access Mode: read_write-deny_delete
Shared Lock is Soft: false
      Delegation Type: -
      Client Address: 192.168.1.5
      SMB Open Type: durable
      SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
      625e2ff46ee5df1194ba0050569d37047058909c00000000873d210700000000

      Vserver: vs0
      Volume: voll
      Logical Interface: node1_data1
      Object Path: /voll/notes.txt
      Lock UUID: 447db185-f801-11df-8bb5-00a098000e34

```

---

---

```

        Lock Protocol: cifs
        Lock Type: op-lock
Node Holding Lock State: node1
        Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
        Oplock Level: read-batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
        Client Address: 192.168.1.5
        SMB Open Type: -
        SMB Connect State: connected
SMB Expiration Time (Secs): -
        SMB Open Group ID:
625e2ff46ee5df1194ba0050569d37047058909c00000000873d210700000000

        Vserver: vs0
        Volume: voll
        Logical Interface: node1_data1
        Object Path: /voll/notes1.txt
        Lock UUID: 48cee334-f801-11df-8bb5-00a098000e34
        Lock Protocol: cifs
        Lock Type: share-level
Node Holding Lock State: node1
        Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
        Oplock Level: -
Shared Lock Access Mode: read_write-deny_delete
Shared Lock is Soft: false
Delegation Type: -
        Client Address: 192.168.1.5
        SMB Open Type: durable
        SMB Connect State: connected
SMB Expiration Time (Secs): -
        SMB Open Group ID:
625e2ff46ee5df1194ba0050569d370440fc8891000000005a3f210700000000
3 entries were displayed.

```

---

---

## vserver name-mapping create

Create a name mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver name-mapping create` command creates a name mapping. Name mappings are applied in the order in which they occur in the priority list; for example, a name mapping that occurs at position 2 in the priority list is applied before a name mapping that occurs at position 3. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list. Data ONTAP prevents you from creating two name mappings with the same pattern.

Patterns can be expressed as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 name mappings in each direction.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression `(.+)` in the CLI, type `"(.+)"` at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to create the name mapping.

**-direction** <Direction of the name mapping> - Name Mapping Direction

This parameter specifies the direction of the name mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX name mapping, `win-unix` for a Windows-to-UNIX name mapping, and `unix-win` for a UNIX-to-Windows name mapping.

**-position** <integer> - Position

This parameter specifies the name mapping's position in the priority list. Specify the position as a positive integer.

Note:

---

If you want to create a new name mapping at a position that is already occupied in the priority list, use the `vserver name-mapping insert` command instead of the `vserver name-mapping create` command.

**-pattern <text>** - Pattern

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

**-replacement <text>** - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.

## Examples

The following example creates a name mapping on a Vserver named `vs1`. The mapping is from UNIX to Windows at position 5 in the priority list. The mapping maps the pattern `cifs` to the replacement `EXAMPLE\Domain Users`.

```
cluster1::> vserver name-mapping create -vserver vs1 -direction unix-win -  
position 5 -pattern cifs -replacement "EXAMPLE\Domain Users"
```

## See Also

`vserver name-mapping insert`

---

## vserver name-mapping delete

Delete a name mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver name-mapping delete` command deletes a name mapping.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to delete the name mapping.

**-direction** <Direction of the name mapping> - Name Mapping Direction

This parameter specifies the direction of the name mapping that you want to delete.

**-position** <integer> - Position

This parameter specifies the position of the name mapping that you want to delete. Specify the position as a positive integer.

### Examples

The following example deletes a name mapping on a Vserver named `vs1`. The name mapping is from UNIX to Windows and is at position 5.

```
cluster1::> vserver name-mapping delete -vserver vs1 -direction unix-win -  
position 5
```

## vserver name-mapping insert

Create a name mapping at a specified position

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver name-mapping insert` command creates a name mapping at a specified position in the priority list. The command rearranges the list as needed to accommodate the new entry. For instance, if you have a priority list of five mappings

---

and insert a new mapping at position 3, the mapping previously at position 3 is moved to position 4, the mapping previously at position 4 is moved to position 5, and the mapping previously at position 5 is moved to position 6. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

You can specify patterns as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 name mappings in each direction.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression `(.+) in the CLI, type "(.+) at the command prompt. To add a "?" to the expression, press ESC followed by the "?".`

## Parameters

**-vserver** <vserver> - Vserver

This parameter specifies the Vserver on which you want to create the name mapping.

**-direction** <Direction of the name mapping> - Name Mapping Direction

This parameter specifies the direction of the name mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX name mapping, `win-unix` for a Windows-to-UNIX name mapping, and `unix-win` for a UNIX-to-Windows name mapping.

**-position** <integer> - Position

This parameter specifies the position in the priority list at which you want to insert the new name mapping. Specify a position as a positive integer.

**-pattern** <text> - Pattern

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

**-replacement** <text> - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.

## Examples

The following example creates a name mapping on a Vserver named `vs1`. It is a user mapping from Kerberos to UNIX. It is inserted into the priority list at position 2. The name mapping maps any principal in the Kerberos realm `SEC.EXAMPLE.COM` to the

---

UNIX user name corresponding to the principal's base name with any instance names removed; for example, tom/admin@SEC.EXAMPLE.COM is mapped to tom.

```
cluster1::> vserver name-mapping insert -vserver vs1 -direction krb-unix -  
position 2 -pattern "([^\@/]+)(/[^\@]+)?@SEC.EXAMPLE.COM" -replacement "\1"
```

## vserver name-mapping modify

Modify a name mapping's pattern, replacement pattern, or both

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver name-mapping modify` command modifies the pattern, the replacement pattern, or both of a specified name mapping.

You can specify patterns as POSIX regular expressions. For information about regular expressions, see the UNIX reference page for `regex(7)`.

Each Vserver can have up to 1024 name mappings in each direction.

Note:

If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression `(.+)` in the CLI, type `"(.+)"` at the command prompt. To add a `"?"` to the expression, press ESC followed by the `"?"`.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to modify the name mapping.

**-direction** <Direction of the name mapping> - Name Mapping Direction

This parameter specifies the direction of the name mapping. Possible values are `krb-unix` for a Kerberos-to-UNIX name mapping, `win-unix` for a Windows-to-UNIX name mapping, and `unix-win` for a UNIX-to-Windows name mapping.

**-position** <integer> - Position

This parameter specifies the name mapping's position in the priority list. A position is specified as a positive integer. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

**[-pattern** <text>] - Pattern

---

This parameter specifies the pattern you want to match. Refer to the command description section for details. The pattern can be up to 256 characters in length.

**[-replacement <text>]** - Replacement

This parameter specifies the replacement pattern. The replacement pattern can be up to 256 characters in length.

## Examples

The following example modifies the name mapping on the Vserver named `vs1` and direction `win-unix`, at position 3. The pattern to be matched is changed to `"EXAMPLE\(.+)"`.

```
cluster1::> vserver name-mapping modify -vserver vs1 -direction win-unix -  
position 3 -pattern "EXAMPLE\(.+)"
```

## vserver name-mapping show

Display name mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver name-mapping show` command displays information about name mappings. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all name mappings:

- Vserver name
- Direction of the mapping (krb-unix for Kerberos-to-UNIX, win-unix for Windows-to-UNIX, or unix-win for UNIX-to-Windows)
- Position of the mapping in the priority list
- Pattern to be matched
- Replacement pattern

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about Kerberos-to-UNIX name mappings, run the command with the `-direction krb-unix` parameter.

## Parameters



---

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the name mapping or mappings that match the specified Vserver.

[-direction <Direction of the name mapping>] - Name Mapping Direction

If you specify this parameter, the command displays information only about the name mapping or mappings that have the specified mapping direction.

[-position <integer>] - Position

If you specify this parameter, the command displays information only about the name mapping that has the specified position in the priority list.

[-pattern <text>] - Pattern

If you specify this parameter, the command displays information only about the name mapping or mappings that use the specified matching pattern. The pattern can be up to 256 characters in length. Refer to the command description section for details.

[-replacement <text>] - Replacement

If you specify this parameter, the command displays information only about the name mapping or mappings that use the specified replacement pattern.

## Examples

The following example displays information about all name mappings:

```
cluster1::> vsriver name-mapping show
Vserver      Direction Position
-----
vs1          win-unix  1      Pattern: EXAMPLE\\administrator
            Replacement: nobody
vs1          unix-win  1      Pattern: EXAMPLE\\(.+)
            Replacement: \_1
vs2          win-unix  1      Pattern: (.+)
            Replacement: EXAMPLE\\administrator
```

---

## vserver name-mapping swap

Exchange the positions of two name mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver name-mapping swap` command exchanges the positions of two name mappings in the priority list.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the name mappings are located.

**-direction** <Direction of the name mapping> - Name Mapping Direction

This parameter specifies the direction of the name mappings that you want to exchange. Each mapping direction (Kerberos-to-UNIX, Windows-to-UNIX, and UNIX-to-Windows) has its own priority list.

**-position** <integer> - Position

This parameter specifies the position in the priority list of the first name mapping that you want to exchange. Specify a position as a positive integer.

**-with-position** <integer> - Position of an existing name mapping entry in the list of name mappings for this Vserver. This entry will be swapped with the entry at 'position'.

This parameter specifies the position in the priority list of the second name mapping that you want to exchange. Specify a position as a positive integer.

### Examples

The following example exchanges the positions of two name mappings on a Vserver named `vs1`. The name mappings have the direction `Windows-to-UNIX`. The name mappings are exchanged between positions 2 and 4.

```
cluster1::> vserver name-mapping swap -vserver vs1 -direction win-unix -position  
2 -with-position 4
```

## vserver nfs create

---

Create an NFS configuration for a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver nfs create` command enables and configures a Vserver to serve NFS clients. The Vserver must already exist. An NFS-enabled Vserver is associated with an NIS domain.

## Parameters

**-vserver** <vserver name> - Vserver

This optional parameter specifies the Vserver on which you want to enable and configure NFS. The default setting is `vs0`.

**[-access {true|false}]** - General NFS Access

This optional parameter specifies whether to enable NFS access on the Vserver. The default setting is `true`.

**[-rpcsec-ctx-high <integer>]** - RPC GSS Context Cache High Water Mark (privilege: advanced)

This optional parameter specifies the maximum number of `RPCSEC_GSS` authentication contexts, which are used by Kerberos. The default setting is zero. See RFC 2203 for information about `RPCSEC_GSS` contexts.

**[-rpcsec-ctx-idle <integer>]** - RPC GSS Context Idle (privilege: advanced)

This optional parameter specifies, in seconds, the amount of time a `RPCSEC_GSS` context is permitted to remain unused before it is deleted. The default setting is zero seconds. See RFC 2203 for information about `RPCSEC_GSS` contexts.

**[-v3 {enabled|disabled}]** - NFS v3

This optional parameter specifies whether to enable access for NFSv3 clients. The default setting is `enabled`.

**[-v4.0 {enabled|disabled}]** - NFS v4.0

This optional parameter specifies whether to enable access for NFSv4.0 clients. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-udp {enabled|disabled}]** - UDP Protocol

---

This optional parameter specifies whether to enable NFS access over UDP. The default setting is `enabled`. This parameter is not supported for Vservers with Infinite Volume.

Note:

Even if UDP is disabled, if TCP is enabled, the Vserver does not block the NFSv3 traffic over UDP. By allowing this traffic, the storage system can process NFS\_NULL ops that the Solaris automounter sends to determine if the storage system is alive. (Solaris sends these ops over UDP even if configured to use TCP.) To block this traffic, you can use export-policy rules to completely disable UDP access. For more information, see the `vserver export-policy rule create` command.

**[-tcp {enabled|disabled}]** - TCP Protocol

This optional parameter specifies whether to enable NFS access over TCP. The default setting is `enabled`.

**[-spinauth {enabled|disabled}]** - Spin Authentication

This optional parameter specifies whether to enable spinauth over NFS. The default setting is `disabled`.

**[-default-win-user <text>]** - Default Windows User

This optional parameter specifies a list of default Windows users for the NFS server.

**[-enable-epsilon {true|false}]** - Enable NFSv3 EJUKEBOX error (privilege: advanced)

This optional parameter specifies whether EJUKEBOX errors are enabled for NFSv3. The default setting is `true`.

**[-v3-require-read-attributes {true|false}]** - Require All NFSv3 Reads to Return Read Attributes (privilege: advanced)

This optional parameter specifies whether NFSv3 read operations are required to return read attributes. The default setting is `false`.

**[-v3-fsid-change {enabled|disabled}]** - Show Change in FSID as NFSv3 Clients Traverse Filesystems (privilege: advanced)

This optional parameter specifies whether Data ONTAP shows changes in file system identifiers (FSIDs) as NFSv3 clients traverse file systems. The default setting is `enabled`.

**[-v3-connection-drop {enabled|disabled}]** - Enable the Dropping of a Connection When an NFSv3 Request is Dropped (privilege: advanced)

This optional parameter specifies whether Data ONTAP allows to drop the connection when a NFSv3 request is dropped. The default setting is `enabled`.

---

**[-ntfs-unix-security-ops <NfsNtfsUnixSecOps>]** - Vserver NTFS Unix Security Options (privilege: advanced)

This optional parameter specifies how NFSv3 security changes affect NTFS volumes. If you set this parameter to `ignore`, Data ONTAP ignores NFSv3 security changes. If you set this parameter to `fail`, NFSv3 security changes fail. If you set this parameter to `use_export_policy`, Data ONTAP processes NFSv3 security changes in accordance with the relevant export rules. The default setting is `use_export_policy`.

**[-chown-mode {restricted|unrestricted|use-export-policy}]** - Vserver Change Ownership Mode (privilege: advanced)

This optional parameter specifies the change ownership mode. The default setting is `use_export_policy`.

**[-trace-enabled {true|false}]** - NFS Response Trace Enabled (privilege: advanced)

This optional parameter specifies whether Data ONTAP logs NFS requests when they exceed the NFS response trigger time (see the `trigger` parameter). The default setting is `false`.

**[-trigger <integer>]** - NFS Response Trigger (in secs) (privilege: advanced)

This optional parameter specifies the amount of time, in seconds, after which Data ONTAP must log an NFS request if it has not completed (assuming the `-trace-enabled` option is `true`). The default setting is 60.

**[-udp-max-xfer-size <integer>]** - UDP Maximum Transfer Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the NFS mount protocol will negotiate with the client for UDP transport. The range is 8192 to 57344. The default setting is 32768.

**[-tcp-max-xfer-size <integer>]** - TCP Maximum Transfer Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv2 and NFSv4 protocols. The range is 8192 to 65536. The default setting is 65536.

**[-v3-tcp-max-read-size <integer>]** - NFSv3 TCP Maximum Read Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv3 read requests. The range is 8192 to 1048576. The default setting is 65536 when created.

Note:

---

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v3-tcp-max-write-size <integer>]** - NFSv3 TCP Maximum Write Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv3 write requests. The range is 8192 to 65536. The default setting is 65536 when created.

Note:

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v4.0-acl {enabled|disabled}]** - NFSv4.0 ACL Support

This optional parameter specifies whether Data ONTAP supports NFSv4.0 access control lists (ACLs). The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.0-read-delegation {enabled|disabled}]** - NFSv4.0 Read Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.0 read delegations. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.0-write-delegation {enabled|disabled}]** - NFSv4.0 Write Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.0 write delegations. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-v4-fsid-change {enabled|disabled}]** - Show Change in FSID as NFSv4 Clients Traverse Filesystems (privilege: advanced)

This optional parameter specifies whether Data ONTAP shows changes in file system identifiers (FSIDs) as NFSv4 clients traverse file systems. The default setting is `enabled`.

Note:

If users access the storage system using NFSv4 from Solaris 10 clients, you must set this option to `disabled`.

**[-v4.0-referrals {enabled|disabled}]** - NFSv4.0 Referral Support (privilege: advanced)

---

This optional parameter specifies whether Data ONTAP supports NFSv4.0 referrals. The default setting is `disabled`. You can set this parameter to `enabled` only if you also set the `-v4-fsid-change` to `enabled`. If clients accessing the node do not support NFSv4.0 referrals, set this option to `disabled`; otherwise, those clients will not be able to access the file system. This parameter is not supported for Vservers with Infinite Volume.

**`[-v4-id-domain <nis domain>]`** - NFSv4 ID Mapping Domain

This optional parameter specifies the domain portion of the string form of user and group names as defined by the NFSv4 protocol. By default, the domain name is normally taken from the NIS domain or the DNS domain in use. However, the value of this parameter overrides the default behavior.

**`[-v4-validate-symlinkdata {enabled|disabled}]`** - NFSv4 Validate UTF-8 Encoding of Symbolic Link Data (privilege: advanced)

This optional parameter specifies whether Data ONTAP validates the UTF-8 encoding of symbolic link data. The default setting is `disabled`.

**`[-v4-lease-seconds <integer>]`** - NFSv4 Lease Timeout Value (in secs) (privilege: advanced)

This optional parameter specifies the time period in which Data ONTAP irrevocably grants a lock to a client. By default, the lease period is 30 seconds. The minimum value is 10. The maximum value is one less than the value of the `-v4-grace-seconds` parameter.

**`[-v4-grace-seconds <integer>]`** - NFSv4 Grace Timeout Value (in secs) (privilege: advanced)

This optional parameter specifies the time period in which clients attempt to reclaim their locking state from Data ONTAP during server recovery. By default, the grace period is 45 seconds. The minimum value is 1 more than the value of the `-v4-lease-seconds` parameter. The maximum value is 90.

**`[-v4-acl-preserve {enabled|disabled}]`** - Preserves and Modifies NFSv4 ACL (privilege: advanced)

This optional parameter specifies if the NFSv4 acl is preserved or dropped when `chmod` is performed. The default is `enabled`.

**`[-v4.1 {enabled|disabled}]`** - NFSv4.1 Minor Version Support

This optional parameter specifies whether to enable access for NFSv4.1 clients. The default setting is `disabled`.

**`-rquota {enabled|disabled}`** - Rquota Enable

---

This optional parameter specifies whether to enable rquota over NFS. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.1-implementation-domain <nis domain>]** - NFSv4.1 Implementation ID Domain (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation domain.

**[-v4.1-implementation-name <text>]** - NFSv4.1 Implementation ID Name (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation name.

**[-v4.1-implementation-date <Date>]** - NFSv4.1 Implementation ID Date (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation date.

**[-v4.1-pnfs {enabled|disabled}]** - NFSv4.1 Parallel NFS Support

This optional parameter specifies whether Data ONTAP supports parallel NFS over NFSv4.1. The default setting is `enabled`.

**[-v4.1-referrals {enabled|disabled}]** - NFSv4.1 Referral Support (privilege: advanced)

This optional parameter specifies whether Data ONTAP supports NFSv4.1 referrals. The default setting is `disabled`. You can set this parameter to `enabled` only if you also set the `-v4-fsid-change` to `enabled`. If clients accessing the node do not support NFSv4.1 referrals, set this option to `disabled`; otherwise, those clients will not be able to access the file system. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.1-acl {enabled|disabled}]** - NFSv4.1 ACL Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 access control lists (ACLs). The default setting is `disabled`.

**[-vstorage {enabled|disabled}]** - NFS vStorage Support

This optional parameter specifies whether to enable vstorage over NFS. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-default-win-group <text>]** - Default Windows Group

This optional parameter specifies a list of default Windows groups for the NFS server.

**[-v4.1-read-delegation {enabled|disabled}]** - NFSv4.1 Read Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 read delegations. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.



---

**[-v4.1-write-delegation {enabled|disabled}]** - NFSv4.1 Write Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 write delegations. The default setting is `disabled`. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.x-session-num-slots <integer>]** - Number of Slots in the NFSv4.x Session slot tables (privilege: advanced)

This optional parameter specifies the number of entries in the NFSv4.x session slot table. By default, the number of slots is 180. The maximum value is 2000.

**[-v4.x-session-slot-reply-cache-size <integer>]** - Size of the Reply that will be Cached in Each NFSv4.x Session Slot (in bytes) (privilege: advanced)

This optional parameter specifies the number of bytes of the reply that will be cached in each NFSv4.x session slot. By default, the size of the cached reply is 640 bytes. The maximum value is 4096.

**[-v4-acl-max-aces <integer>]** - Maximum Number of ACEs per ACL (privilege: advanced)

This optional parameter specifies the maximum number of ACEs in an NFSv4 ACL. The range is 192 to 1024. The default value is 400. Setting it to a value more than the default could cause performance problems for clients accessing files with NFSv4 ACLs.

**[-mount-rootonly {enabled|disabled}]** - NFS Mount Root Only

This optional parameter specifies whether the vserver allows MOUNT protocol calls only from privileged ports (port numbers less than 1024). The default setting is `enabled`.

**[-nfs-rootonly {enabled|disabled}]** - NFS Root Only

This optional parameter specifies whether the vserver allows NFS protocol calls only from privileged ports (port numbers less than 1024). The default setting is `disabled`.

## Examples

The following example enables and configures NFS access on a Vserver named `vs0`. NFS access is enabled. The maximum number of RPCSEC\_GSS authentication contexts is set to 5. The RPCSEC\_GSS idle time is set to 360 seconds. Access is enabled for NFS v3 clients over both UDP and TCP.

```
cluster1::> vserver nfs create -vserver vs0 -access true -rpcsec-ctx-high 5 -  
rpcsec-ctx-idle 360 -v3 enabled -udp enabled -tcp enabled
```

## See Also

`vserver export-policy rule create`

---

## vserver nfs delete

Delete the NFS configuration of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs delete` command deletes the NFS configuration of a specified Vserver. This command does not delete the Vserver itself, just its ability to serve NFS clients.

Note:

If you delete a Vserver, the Vserver's NFS configuration is automatically deleted. Any Windows-to-UNIX or UNIX-to-Windows name mappings defined for the Vserver are also deleted because they require both the CIFS and NFS servers.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver whose NFS configuration you want to delete.

### Examples

The following example deletes the NFS configuration of a Vserver named vs2:

```
cluster1::> vserver nfs delete -vserver vs2
```

## vserver nfs modify

Modify the NFS configuration of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs modify` command modifies the configuration of an NFS-enabled Vserver.

---

## Parameters

**-vserver** <vserver name> - Vserver

This specifies the Vserver whose NFS configuration you want to modify.

**[-access {true|false}]** - General NFS Access

This optional parameter specifies whether NFS access is enabled on the Vserver.

**[-rpcsec-ctx-high <integer>]** - RPC GSS Context Cache High Water Mark (privilege: advanced)

This optional parameter specifies the maximum number of RPCSEC\_GSS authentication contexts, which are used by Kerberos. The default setting is zero at the time of creation. See RFC 2203 for information about RPCSEC\_GSS contexts.

**[-rpcsec-ctx-idle <integer>]** - RPC GSS Context Idle (privilege: advanced)

This optional parameter specifies, in seconds, the amount of time a RPCSEC\_GSS context is permitted to remain unused before it is deleted. The default setting is zero seconds at the time of creation. See RFC 2203 for information about RPCSEC\_GSS contexts.

**[-v3 {enabled|disabled}]** - NFS v3

This optional parameter specifies whether to enable access for NFS v3 clients.

**[-v4.0 {enabled|disabled}]** - NFS v4.0

This optional parameter specifies whether to enable access for NFSv4.0 clients. The default setting is *enabled* at the time of creation. This parameter is not supported for Vservers with Infinite Volume.

**[-udp {enabled|disabled}]** - UDP Protocol

This optional parameter specifies whether to enable NFS access over UDP. This value is not modifiable on a Vserver with Infinite Volume.

Note:

Even if UDP is disabled, if TCP is enabled, the Vserver does not block the NFSv3 traffic over UDP. By allowing this traffic, the storage system can process NFS\_NULL ops that the Solaris automounter sends to determine if the storage system is alive. (Solaris sends these ops over UDP even if configured to use TCP.) To block this traffic, you can use export-policy rules to completely disable UDP access. For more information, see the `vserver export-policy rule create` command.

**[-tcp {enabled|disabled}]** - TCP Protocol

---

This optional parameter specifies whether to enable NFS access over TCP.

**[-spinauth {enabled|disabled}]** - Spin Authentication

This optional parameter specifies whether to enable spinauth over NFS.

**[-default-win-user <text>]** - Default Windows User

This optional parameter specifies a list of default Windows users for the NFS server.

**[-enable-ejukebox {true|false}]** - Enable NFSv3 EJUKEBOX error (privilege: advanced)

This optional parameter specifies whether EJUKEBOX errors are enabled for NFSv3. The default setting is `true` at the time of creation.

**[-v3-require-read-attributes {true|false}]** - Require All NFSv3 Reads to Return Read Attributes (privilege: advanced)

This optional parameter specifies whether NFSv3 read operations are required to return read attributes. The default setting is `false` at the time of creation.

**[-v3-fsid-change {enabled|disabled}]** - Show Change in FSID as NFSv3 Clients Traverse Filesystems (privilege: advanced)

This optional parameter specifies whether Data ONTAP shows changes in file system identifiers (FSIDs) as NFSv3 clients traverse file systems. If you change the value of this parameter, clients must remount any paths over which they are using NFSv3.

**[-v3-connection-drop {enabled|disabled}]** - Enable the Dropping of a Connection When an NFSv3 Request is Dropped (privilege: advanced)

This optional parameter specifies whether NFS v3 connection drop is enabled. The default setting is `enabled` at the time of creation.

**[-ntfs-unix-security-ops <NfsNtfsUnixSecOps>]** - Vserver NTFS Unix Security Options (privilege: advanced)

This optional parameter specifies how NFSv3 security changes affect NTFS volumes. If you set this parameter to `ignore`, Data ONTAP ignores NFSv3 security changes. If you set this parameter to `fail`, NFSv3 security changes fail. If you set this parameter to `use_export_policy`, Data ONTAP processes NFSv3 security changes in accordance with the relevant export rules. The default setting is `ignore` at the time of creation.

**[-chown-mode {restricted|unrestricted|use-export-policy}]** - Vserver Change Ownership Mode (privilege: advanced)

This optional parameter specifies whether ownership of a file can be changed by superusers or by non-root users who currently own the file. If you set this parameter to `restricted`, the ownership of a file can be changed by superusers only. If you set this parameter to `unrestricted`, the ownership of a file can be changed by superusers

---

and the current owner of the file. If you set this parameter to `use-export-policy`, the ownership of a file can be changed in accordance with the relevant export rules.

**[-trace-enabled {true|false}]** - NFS Response Trace Enabled (privilege: advanced)

This optional parameter specifies whether Data ONTAP logs NFS requests when they exceed the NFS response trigger time (see the `trigger` parameter). The default setting is `false` at the time of creation.

**[-trigger <integer>]** - NFS Response Trigger (in secs) (privilege: advanced)

This optional parameter specifies the amount of time, in seconds, after which Data ONTAP must log an NFS request if it has not completed (assuming the `-trace-enabled` option is set to `true`). The default setting is 60 at the time of creation.

**[-udp-max-xfer-size <integer>]** - UDP Maximum Transfer Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the NFS mount protocol negotiates with the client for UDP transport. The range is 8192 to 57344. The default setting is 32768 at the time of creation.

**[-tcp-max-xfer-size <integer>]** - TCP Maximum Transfer Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv2 and NFSv4 protocols. The range is 8192 to 65536. The default setting is 65536 when created.

**[-v3-tcp-max-read-size <integer>]** - NFSv3 TCP Maximum Read Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv3 read requests. The range is 8192 to 1048576. The default setting is 65536 when created.

Note:

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v3-tcp-max-write-size <integer>]** - NFSv3 TCP Maximum Write Size (privilege: advanced)

This optional parameter specifies the maximum transfer size (in bytes) that the storage system negotiates with the client for TCP transport of data for NFSv3 write requests. The range is 8192 to 65536. The default setting is 65536 when created.

Note:

---

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v4.0-acl {enabled|disabled}] - NFSv4.0 ACL Support**

This optional parameter specifies whether Data ONTAP supports NFSv4.0 access control lists (ACLs). The default setting is `disabled` when created. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.0-read-delegation {enabled|disabled}] - NFSv4.0 Read Delegation Support**

This optional parameter specifies whether Data ONTAP supports NFSv4 read delegations. The default setting is `disabled` when created. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.0-write-delegation {enabled|disabled}] - NFSv4.0 Write Delegation Support**

This optional parameter specifies whether Data ONTAP supports NFSv4 write delegations. The default setting is `disabled` when created. This parameter is not supported for Vservers with Infinite Volume.

**[-v4-fsid-change {enabled|disabled}] - Show Change in FSID as NFSv4 Clients Traverse Filesystems (privilege: advanced)**

This optional parameter specifies whether Data ONTAP shows changes in file system identifiers (FSIDs) as NFSv4 clients traverse file systems. The default setting is `enabled` when created. If you change the value of this parameter, clients must remount any paths over which they are using NFSv4.

Note:

If users access the storage system using NFSv4 from Solaris 10 clients, you must set this option to `disabled`.

**[-v4.0-referrals {enabled|disabled}] - NFSv4.0 Referral Support (privilege: advanced)**

This optional parameter specifies whether Data ONTAP supports NFSv4.0 referrals. The default setting is `disabled` when created. You can set this parameter to `enabled` only if the `-v4-fsid-change` option is also set to `enabled`. If clients accessing the node do not support NFSv4.0 referrals, set this option to `disabled`; otherwise, those clients will not be able to access the file system. This parameter is not supported for Vservers with Infinite Volume.

**[-v4-id-domain <nis domain>] - NFSv4 ID Mapping Domain**

This optional parameter specifies the domain portion of the string form of user and group names as defined by the NFSv4 protocol. By default, the domain name is

---

normally taken from the NIS domain or the DNS domain in use. However, the value of this parameter overrides the default behavior.

**[-v4-validate-symlinkdata {enabled|disabled}]** - NFSv4 Validate UTF-8 Encoding of Symbolic Link Data (privilege: advanced)

This optional parameter specifies whether Data ONTAP validates the UTF-8 encoding of symbolic link data. The default setting is `disabled` when created.

**[-v4-lease-seconds <integer>]** - NFSv4 Lease Timeout Value (in secs) (privilege: advanced)

This optional parameters specifies the time period in which Data ONTAP irrevocably grants a lock to a client. By default, the lease period is 30 seconds. The minimum value is 10. The maximum value is one less than the value of the `-v4-grace-seconds` parameter.

**[-v4-grace-seconds <integer>]** - NFSv4 Grace Timeout Value (in secs) (privilege: advanced)

This optional parameter specifies the time period in which clients attempt to reclaim their locking state from Data ONTAP during server recovery. By default, the grace period is 45 seconds. The minimum value is 1 more than the value of the `-v4-lease-seconds` parameter. The maximum value is 90.

**[-v4-acl-preserve {enabled|disabled}]** - Preserves and Modifies NFSv4 ACL (privilege: advanced)

This optional parameter specifies if the NFSv4 acl is preserved or dropped when `chmod` is performed. The default is `enabled`.

**[-v4.1 {enabled|disabled}]** - NFSv4.1 Minor Version Support

This optional parameter specifies whether to enable access for NFSv4.1 clients. The default setting is `enabled` at the time of creation.

**[-rquota {enabled|disabled}]** - Rquota Enable

This optional parameter specifies whether to enable rquota over NFS. The default setting is `disabled` at the time of creation. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.1-implementation-domain <nis domain>]** - NFSv4.1 Implementation ID Domain (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation domain.

**[-v4.1-implementation-name <text>]** - NFSv4.1 Implementation ID Name (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation name.

---

**[-v4.1-implementation-date <Date>]** - NFSv4.1 Implementation ID Date (privilege: advanced)

This optional parameter specifies the NFSv4.1 implementation date.

**[-v4.1-pnfs {enabled|disabled}]** - NFSv4.1 Parallel NFS Support

This optional parameter specifies whether to enable access for pNFS for NFSv4.1. The default setting is `enabled` at the time of creation.

**[-v4.1-referrals {enabled|disabled}]** - NFSv4.1 Referral Support (privilege: advanced)

This optional parameter specifies whether Data ONTAP supports NFSv4.1 referrals. The default setting is `disabled` when created. You can set this parameter to `enabled` only if the `-v4-fsid-change` option is also set to `enabled`. If clients accessing the node do not support NFSv4.1 referrals, set this option to `disabled`; otherwise, those clients will not be able to access the file system. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.1-acl {enabled|disabled}]** - NFSv4.1 ACL Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 access control lists (ACLs). The default setting is `disabled` when created.

**[-vstorage {enabled|disabled}]** - NFS vStorage Support

This optional parameter specifies whether to enable vstorage over NFS. The default setting is `disabled` at the time of creation. This parameter is not supported for Vservers with Infinite Volume.

**[-default-win-group <text>]** - Default Windows Group

This optional parameter specifies a list of default Windows groups for the NFS server.

**[-v4.1-read-delegation {enabled|disabled}]** - NFSv4.1 Read Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 read delegations. The default setting is `disabled` when created. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.1-write-delegation {enabled|disabled}]** - NFSv4.1 Write Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 write delegations. The default setting is `disabled` when created. This parameter is not supported for Vservers with Infinite Volume.

**[-v4.x-session-num-slots <integer>]** - Number of Slots in the NFSv4.x Session slot tables (privilege: advanced)

This optional parameter specifies the number of entries in the NFSv4.x session slot table. By default, the number of slots is 180. The maximum value is 2000.



---

**[-v4.x-session-slot-reply-cache-size <integer>]** - Size of the Reply that will be Cached in Each NFSv4.x Session Slot (in bytes) (privilege: advanced)

This optional parameter specifies the number of bytes of the reply that will be cached in each NFSv4.x session slot. By default, the size of the cached reply is 640 bytes. The maximum value is 4096.

**[-v4-acl-max-aces <integer>]** - Maximum Number of ACEs per ACL (privilege: advanced)

This optional parameter specifies the maximum number of ACEs in a NFSv4 ACL. The range is 192 to 1024. The default value is 400. Setting it to a value more than the default could cause performance problems for clients accessing files with NFSv4 ACLs.

**[-mount-rootonly {enabled|disabled}]** - NFS Mount Root Only

This optional parameter specifies whether the vserver allows MOUNT protocol calls only from privileged ports (port numbers less than 1024). The default setting is `enabled`.

**[-nfs-rootonly {enabled|disabled}]** - NFS Root Only

This optional parameter specifies whether the vserver allows NFS protocol calls only from privileged ports (port numbers less than 1024). The default setting is `disabled`.

## Examples

The following example enables NFS access on a Vserver named `vs0` for NFS clients that use NFS v3 over TCP:

```
cluster1::> vserver nfs modify -vserver vs0 -access true -v3 enabled -udp
disabled -tcp enabled
```

## See Also

`vserver export-policy rule create`

---

## vserver nfs off

Disable the NFS service of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs off` command disables NFS access on a Vserver. The Vserver must already exist.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to disable NFS access.

### Examples

The following example disables NFS access on a Vserver named vs0.

```
cluster1::> vserver nfs off -vserver vs0
```

## vserver nfs on

Enable the NFS service of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs on` command enables NFS access on a Vserver. The Vserver must already exist.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to enable NFS access.

### Examples

---

The following example enables NFS access on a Vserver named vs0.

```
cluster1::> vserver nfs on -vserver vs0
```

## vserver nfs show

Display the NFS configurations of Vservers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs show` command displays information about NFS-enabled Vservers. The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all NFS-enabled Vservers:

- Vserver name
- Whether general NFS access is enabled
- Whether access to NFSv3 clients is enabled
- Whether access to NFSv4 clients is enabled
- Whether NFS access over UDP is enabled
- Whether NFS access over TCP is enabled
- List of default Windows users (detailed view only)

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about Vservers that enable access over TCP, enter the command with the `-tcp-enable true` parameter.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| **[-krb-opts ]** (privilege: advanced)

If you specify the parameter for `-instance`, the command shows detailed information about all NFS-enabled Vservers. Otherwise, if the `-krb-opts` parameter is specified, the command shows the following Kerberos-related information:

- Vserver name
- Maximum number of RPCSEC\_GSS authentication contexts
- Time, in seconds, an RPCSEC\_GSS context can remain idle before being deleted

Otherwise, if the `-fields` parameter is specified, the command shows information about all of the NFS-enabled Vservers that you specify as a comma-delimited list.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays information only about the specified NFS-enabled Vserver.

**[-access {true|false}]** - General NFS Access

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified general-access setting.

**[-rpcsec-ctx-high <integer>]** - RPC GSS Context Cache High Water Mark (privilege: advanced)

If you specify this parameter, the command displays information only about NFS-enabled Vservers that have the specified maximum number of RPCSEC\_GSS authentication contexts.

**[-rpcsec-ctx-idle <integer>]** - RPC GSS Context Idle (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified timeout value for idle RPCSEC\_GSS contexts.

**[-v3 {enabled|disabled}]** - NFS v3

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv3 is enabled or disabled.

**[-v4.0 {enabled|disabled}]** - NFS v4.0

If you specify this parameter, the command displays information only about NFS-enabled Vservers for which NFSv4.0 is enabled or disabled.

**[-udp {enabled|disabled}]** - UDP Protocol

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified NFS-over-UDP access setting.

**[-tcp {enabled|disabled}]** - TCP Protocol

---

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified NFS-over-TCP setting.

**[-spinauth {enabled|disabled}]** - Spin Authentication

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which spinauth is enabled or disabled.

**[-default-win-user <text>]** - Default Windows User

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified list of default Windows users.

**[-enable-ejukebox {true|false}]** - Enable NFSv3 EJUKEBOX error (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which EJUKEBOX errors are enabled or disabled.

**[-v3-require-read-attributes {true|false}]** - Require All NFSv3 Reads to Return Read Attributes (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv3 read operations are required or not required to return read attributes.

**[-v3-fsid-change {enabled|disabled}]** - Show Change in FSID as NFSv3 Clients Traverse Filesystems (privilege: advanced)

If you specify this parameter, the command displays information about changes in file system identifiers (FSIDs) as NFSv3 clients traverse file systems.

**[-v3-connection-drop {enabled|disabled}]** - Enable the Dropping of a Connection When an NFSv3 Request is Dropped (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv3 connection-drop is enabled or disabled.

**[-ntfs-unix-security-ops <NfsNtfsUnixSecOps>]** - Vserver NTFS Unix Security Options (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the NTFS-UNIX security setting is `ignore`, `fail`, or `use_export_policy`.

**[-chown-mode {restricted|unrestricted|use-export-policy}]** - Vserver Change Ownership Mode (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which chown-mode setting is `restricted`, `unrestricted`, or `use_export_policy`.

---

**[-trace-enabled {true|false}]** - NFS Response Trace Enabled (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which tracing is enabled or disabled.

**[-trigger <integer>]** - NFS Response Trigger (in secs) (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers with the specified NFS response trigger time.

**[-udp-max-xfer-size <integer>]** - UDP Maximum Transfer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers with the specified UDP maximum transfer size. The range is 8192 to 57344.

**[-tcp-max-xfer-size <integer>]** - TCP Maximum Transfer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers with the specified TCP maximum transfer size. The range is 8192 to 65536.

**[-v3-tcp-max-read-size <integer>]** - NFSv3 TCP Maximum Read Size (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers with the specified TCP maximum transfer size for NFSv3 read requests. The range is 8192 to 1048576.

Note:

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v3-tcp-max-write-size <integer>]** - NFSv3 TCP Maximum Write Size (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers with the specified TCP maximum transfer size for NFSv3 write requests. The range is 8192 to 65536.

Note:

This field is supported only if all the nodes in the cluster are running Data ONTAP version 8.1.0 or later.

**[-v4.0-acl {enabled|disabled}]** - NFSv4.0 ACL Support

---

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4 ACLs have been enabled or disabled.

**[-v4.0-read-delegation {enabled|disabled}]** - NFSv4.0 Read Delegation Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4 read delegation has been enabled or disabled.

**[-v4.0-write-delegation {enabled|disabled}]** - NFSv4.0 Write Delegation Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4 write delegation has been enabled or disabled.

**[-v4-fsid-change {enabled|disabled}]** - Show Change in FSID as NFSv4 Clients Traverse Filesystems (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the showing of NFSv4 file system identifier (FSID) changes has been enabled or disabled.

**[-v4.0-referrals {enabled|disabled}]** - NFSv4.0 Referral Support (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.0 referrals have been enabled or disabled.

**[-v4-id-domain <nis domain>]** - NFSv4 ID Mapping Domain

If you specify this parameter, the command displays information only about the NFS-enabled Vservers having the specified NIS domain.

**[-v4-validate-symlinkdata {enabled|disabled}]** - NFSv4 Validate UTF-8 Encoding of Symbolic Link Data (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which validation of UTF-8 encoding of symbolic link data has been enabled or disabled.

**[-v4-lease-seconds <integer>]** - NFSv4 Lease Timeout Value (in secs) (privilege: advanced)

If you specify this parameter, it displays the locking lease period. It is expressed in seconds. Clients that have been inactive for a period equal or longer to the lease period may lose all their locking state on a node.

**[-v4-grace-seconds <integer>]** - NFSv4 Grace Timeout Value (in secs) (privilege: advanced)

If you specify this parameter, it displays the grace period for clients to reclaim file locks after a server failure. The grace period is expressed in seconds.

---

**[-v4-acl-preserve {enabled|disabled}]** - Preserves and Modifies NFSv4 ACL (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4 ACL preserve has been enabled or disabled.

**[-v4.1 {enabled|disabled}]** - NFSv4.1 Minor Version Support

If you specify this parameter, the command displays information only about NFS-enabled Vservers for which NFSv4.1 is enabled or disabled.

**[-rquota {enabled|disabled}]** - Rquota Enable

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which rquota has been enabled or disabled.

**[-v4.1-implementation-domain <nfs domain>]** - NFSv4.1 Implementation ID Domain (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 implementation domain has been enabled or disabled.

**[-v4.1-implementation-name <text>]** - NFSv4.1 Implementation ID Name (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 implementation name has been enabled or disabled.

**[-v4.1-implementation-date <Date>]** - NFSv4.1 Implementation ID Date (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 implementation date has been enabled or disabled.

**[-v4.1-pnfs {enabled|disabled}]** - NFSv4.1 Parallel NFS Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 pnfs has been enabled or disabled.

**[-v4.1-referrals {enabled|disabled}]** - NFSv4.1 Referral Support (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 referrals have been enabled or disabled.

**[-v4.1-acl {enabled|disabled}]** - NFSv4.1 ACL Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 ACLs have been enabled or disabled.



---

**[-vstorage {enabled|disabled}]** - NFS vStorage Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which vstorage is enabled or disabled.

**[-default-win-group <text>]** - Default Windows Group

If you specify this parameter, the command displays information only about the NFS-enabled Vservers that have the specified list of default Windows groups.

**[-v4.1-read-delegation {enabled|disabled}]** - NFSv4.1 Read Delegation Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 read delegation has been enabled or disabled.

**[-v4.1-write-delegation {enabled|disabled}]** - NFSv4.1 Write Delegation Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which NFSv4.1 write delegation has been enabled or disabled.

**[-v4.x-session-num-slots <integer>]** - Number of Slots in the NFSv4.x Session slot tables (privilege: advanced)

If you specify this parameter, this command displays the number of slots in the NFSv4.x session slot table. The range is 1 to 2000.

**[-v4.x-session-slot-reply-cache-size <integer>]** - Size of the Reply that will be Cached in Each NFSv4.x Session Slot (in bytes) (privilege: advanced)

If you specify this parameter, this command displays the size of the reply that will be cached in each NFSv4.x session slot. The cache size is expressed in bytes. The range is 512 to 4096.

**[-v4-acl-max-aces <integer>]** - Maximum Number of ACEs per ACL (privilege: advanced)

If you specify this parameter, the command sets the maximum number of ACEs that can be set or retrieved on a NFSv4 ACL.

**[-mount-rootonly {enabled|disabled}]** - NFS Mount Root Only

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which mount-rootonly has been enabled or disabled.

**[-nfs-rootonly {enabled|disabled}]** - NFS Root Only

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which nfs-rootonly has been enabled or disabled.

## Examples

The following example displays information about all NFS-enabled Vservers:

```
cluster1::> vserver nfs show
Vserver      General Access  v3      v4      v4.1    UDP      TCP      Default Windows User
-----
vs0          true    enabled disabled disabled enabled enabled -
vs1          true    enabled disabled disabled enabled enabled -
2 entries were displayed.
```

The following example displays Kerberos-related information about all NFS-enabled Vservers:

```
cluster::*> vserver nfs show -krb-opts
Vserver Context High Context Idle
-----
vs0          30          30
vs1          30          30
2 entries were displayed.
```

---

## vserver nfs start

Start the NFS service of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs start` command starts the NFS service on a Vserver to serve NFS clients. The Vserver must already exist.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to start the NFS service.

### Examples

The following example starts the NFS service on a Vserver named vs0.

```
cluster1::> vserver nfs start -vserver vs0
```

## vserver nfs status

Display the status of the NFS service of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs status` command shows the status of NFS on a Vserver. The Vserver must already exist.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which you want to see the NFS status.

**[-is-enabled {true|false}]** - NFS Service Enabled

---

If you specify this optional parameter, the command displays whether NFS is enabled or not. This parameter is true if the NFS server is running.

## Examples

The following example shows the status of NFS on a Vserver named vs0 for which NFS is enabled.

```
cluster1::> vserver nfs status -vserver vs0.  
The NFS server is running.
```

## vserver nfs stop

Stop the NFS service of a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver nfs stop` command stops the NFS service on a Vserver to serve NFS clients. The Vserver must already exist.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to stop the NFS service.

## Examples

The following example stops the NFS service on a Vserver named vs0.

```
cluster1::> vserver nfs stop -vserver vs0
```

## vserver nfs kerberos-config modify

Modify the Kerberos configuration of an NFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

---

The `vserver nfs kerberos-config modify` command modifies a Kerberos configuration for NFS. An NFS Kerberos configuration is associated with both a Vserver and a logical interface.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver associated with the NFS Kerberos configuration you want to modify.

**-lif** <lif-name> - Logical Interface

This parameter specifies the name of the logical interface associated with the NFS Kerberos configuration you want to modify.

**[-kerberos {enabled|disabled}]** - Kerberos Enabled

This optional parameter specifies whether to enable or disable Kerberos for NFS on the specified Vserver and logical interface. If you specify a value of `enable`, you must also specify the `-spn` parameter. The command prompts you for a user name and password for a Kerberos principal in the same realm as the principal specified by the `-spn` parameter; this principal must have permission to create or modify the principal specified by the `-spn` parameter.

**[-spn <text>]** - Service Principal Name

This optional parameter specifies the service principal name (SPN) of the Kerberos configuration you want to modify. If you specify a value of `enable` for the `-kerberos` parameter, you must also specify this parameter. This value must be in the form `nfs/host_name@REALM`, where `host_name` is the fully qualified host name of the Kerberos server, `nfs` is the service, and `REALM` is the name of the Kerberos realm (for instance, `EXAMPLE.COM`). Specify Kerberos realm names in uppercase.

**[-admin-username <text>]** - Account Creation Username

This optional parameter specifies the administrator user name.

**[-keytab-uri {(ftp|http)://(hostname|IPv4 Address|'IPv6 Address')}...}]** - Load keytab from URI

This optional parameter specifies loading a keytab file from the specified URI.

## Examples

The following example enables an NFS Kerberos configuration on a Vserver named `vs0` and a logical interface named `datalif1`. The SPN is `nfs/sec.example.com@AUTH.SEC.EXAMPLE.COM` and the keytab file is loaded from `ftp://ftp.example.com/keytab`.

---

```
vs1::> vserver nfs kerberos-config modify -vserver vs0 -lif datalif1
-kerberos enabled -spn nfs/sec.example.com@AUTH.SEC.EXAMPLE.COM -keytab-uri
ftp://ftp.example.com/keytab
```

---

## vserver nfs kerberos-config show

Display the Kerberos configurations of NFS servers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver nfs kerberos-config show` command displays information about Kerberos configurations for NFS. The command output depends on the parameters specified with the command. If you do not specify any parameters, the command displays the following information about all Kerberos configurations for NFS:

- Vserver name
- Logical interface name
- Logical interface IP address
- Whether Kerberos is enabled or disabled
- The Kerberos service principal name (SPN)
- The configuration's numeric ID

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about Kerberos configurations for NFS that are enabled, run the command with the `-kerberos enabled` parameter.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

---

If you specify this parameter and the `-lif` parameter, the command displays information only about the Kerberos configuration or configurations for NFS that are associated with the specified Vserver and logical interface.

**[`-lif <lif-name>`]** - Logical Interface

If you specify this parameter and the `-vserver` parameter, the command displays information only about the Kerberos configuration or configurations for NFS that are associated with the specified logical interface and Vserver.

**[`-address <IP Address>`]** - IP Address

If you specify this parameter, the command displays information only about the Kerberos configurations for NFS that are associated with the specified logical-interface IP address.

**[`-kerberos {enabled|disabled}`]** - Kerberos Enabled

If you specify this parameter, the command displays information only about the Kerberos configurations for NFS that match the specified value.

**[`-spn <text>`]** - Service Principal Name

If you specify this parameter, the command displays information only about the Kerberos configuration or configurations for NFS that match the specified SPN.

## Examples

The following example displays information about the Kerberos configuration for NFS associated with the Vserver `vs0` and the logical interface `datalif1`:

```
vs1::> vserver nfs kerberos-config show -vserver vs0 -lif datalif1
Logical Interface:      datalif1
LIF IP Address:        192.0.2.130
Kerberos Enabled:      Enabled
Service Principal Name: nfs/sec.example.com@AUTH.SEC.EXAMPLE.COM
```



---

## vserver peer accept

Accept a pending Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer accept` command is used to accept the Vserver peer relationship between two Vservers. This command is used only for intercluster Vserver peer relationships.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies name of the local Vserver for which you want to accept the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies name of the peer Vserver with which the Vserver peer relationship was initiated.

### Examples

The following example illustrates how to accept the Vserver peer relationship between Vservers `pvs1.example.com` residing on Cluster2, and `lvs1.example.com` residing on Cluster1.

```
Cluster2::> vserver peer accept -vserver pvs1.example.com -peer-vserver  
lvs1.example.com
```

### See Also

`vserver peer create` `vserver peer reject`

---

## vserver peer create

Create a new Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer create` command creates a Vserver peer relationship between two Vservers residing on the same cluster or across two clusters. For intercluster Vserver peer relationships, the cluster administrator must accept or reject the relationship on peer cluster.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies the name of the local Vserver.

**-peer-vserver** <text> - Peer Vserver Name

Specifies the name of the peer Vserver with which you want to create the Vserver peer relationship.

**[-peer-cluster** <text>] - Peer Cluster Name

Specifies the name of the peer cluster. If this is not specified, it is assumed that the peer Vserver resides on the same cluster.

**-applications** <snapmirror>, ... - Peering Applications

Specifies the applications for which the Vserver peer relationship is created.

### Examples

The following example illustrates how to create an intercluster Vserver peer relationship between Vserver `lvs1.example.com`, residing on Cluster1, and `pvs1.example.com`, residing on Cluster2. The relationship is created for SnapMirror.

```
Cluster1::> vserver peer create -vserver lvs1.example.com -peer-vserver  
pvs1.example.com -peer-cluster Cluster2 -applications snapmirror
```

Here is another example which creates an intracuster Vserver peer relationship.

```
Cluster1::> vserver peer create -vserver lvs1.example.com -peer-vserver  
lvs2.example.com -applications snapmirror
```

### See Also

---

vserver peer accept   vserver peer reject

---

## vserver peer delete

Delete a Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer delete` command deletes the Vserver peer relationship between two Vservers. The peering state is updated on the peer cluster.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies the local Vserver name for which you want to delete the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies the peer Vserver name with which the Vserver peer relationship was established.

**[-force [true]]** - Force Delete

Deletes the Vserver peer relationship even if the remote cluster is not accessible due to, for example, network connectivity issues.

### Examples

The following example illustrates how to delete the Vserver peer relationship between two Vservers `lvs1.example.com` residing on Cluster1, and `pvs1.example.com` residing on Cluster2.

```
Cluster1::> vserver peer delete -vserver lvs1.example.com -peer-vserver  
pvs1.example.com
```

### See Also

`vserver peer create`

---

## vserver peer modify

Modify a Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer modify` command modifies applications of the Vserver peer relationship.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies name of the local Vserver for which you want to modify applications of the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies name of the peer Vserver for which you want to modify applications of the Vserver peer relationship.

**-applications** <snapmirror>, ... - Peering Applications

Specifies the Vserver peer applications.

### Examples

The following example illustrates how to modify applications that are part of the peer relationship between the Vservers `lvs1.example.com` residing on Cluster1, and `pvs1.example.com` residing on Cluster2.

```
Cluster1::> vserver peer modify -vserver lvs1.example.com -peer-vserver  
pvs1.example.com -applications snapmirror
```

### See Also

`vserver peer create` `vserver peer delete`

---

## vserver peer reject

Reject a Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer reject` command is used to reject the Vserver peer relationship between the two Vservers. This command is used only for an intercluster Vserver peer relationship.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies the name of the local Vserver for which you want to reject the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies the name of the peer Vserver with which the Vserver peer relationship was initiated.

### Examples

The following example illustrates how to reject the Vserver peer relationship between two Vservers `lvs1.example.com` residing on Cluster1, and `pvs1.example.com` residing on Cluster2.

```
Cluster1::> vserver peer reject -vserver lvs1.example.com -peer-vserver  
pvs1.example.com
```

### See Also

`vserver peer create` `vserver peer accept`

---

## vserver peer resume

Resume a Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer resume` command resumes the Vserver peer relationship between two Vservers.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies name of the local Vserver for which you want to resume the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies name of the peer Vserver with which you want to resume the Vserver peer relationship.

**[-force [true]]** - Force Resume

Resumes the Vserver peer relationship even if the remote cluster is not accessible due to, for example, network connectivity issues.

### Examples

The following example illustrates resuming a Vserver peer relationship between two Vservers `lvs1.example.com` residing on Cluster1, and `pvs1.example.com` residing on Cluster2.

```
Cluster1::> vserver peer resume -vserver lvs1.example.com -peer-vserver  
pvs1.example.com
```

### See Also

`vserver peer suspend`

---

## vserver peer show-all

Display Vserver peer relationships in detail

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer show-all` command displays the following information about Vserver peer relationships:

- Local Vserver name
- Peer Vserver name
- Peer cluster name
- Applications
- State of the peering relationship

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver>] - Local Vserver Name

If this parameter is specified, the command displays relationships that match the specified local Vserver.

[-**peer-vserver** <text>] - Peer Vserver Name

If this parameter is specified, the command displays relationships that match the specified peer Vserver.

[-**peer-state** {peered|pending|initializing|initiated|rejected|suspended|deleted}] - Peering State



---

If this parameter is specified, the command displays relationships that match the specified peer state.

**[-applications <snapmirror>, ...]** - Peering Applications

If this parameter is specified, the command displays relationships that have the specified applications.

**[-peer-cluster <text>]** - Peer Cluster Name

If this parameter is specified, the command displays relationships that have the specified peer cluster name.

**Examples**

The following example illustrates how to display Vserver peer relationships.

```
Cluster1::> vserver peer show-all
Vserver      Peer      Peer      Peer Cluster      Peering
-----      -
lvsl.example.com      lvsl2.example.com      peered      Cluster1      snapmirror
lvsl.example.com      pvs1.example.com      peered      sreev-vsim6      snapmirror
lvsl2.example.com      lvsl1.example.com      peered      Cluster1      snapmirror
3 entries were displayed.
```

**See Also**

vserver peer show

---

## vserver peer show

Display Vserver peer relationships

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver peer show` command displays the following information about Vserver peer relationships:

- Local Vserver name
- Peer Vserver name
- State of the peering relationship

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver>] - Local Vserver Name

If this parameter is specified, the command displays information about the specified local Vserver.

[-**peer-vserver** <text>] - Peer Vserver Name

If this parameter is specified, the command displays information about the specified peer Vserver.

[-**peer-state** {peered|pending|initializing|initiated|rejected|suspended|deleted}] - Peering State

If this parameter is specified, the command displays relationships that match the specified peer state.

---

## Examples

The following examples illustrates how to display Vserver peer relationships. Cluster administrator:

```
Cluster1::> vservers peer show
Vserver      Peer      Peer
              Vserver    State
-----
lvsl.example.com
              lvs2.example.com
                      peer
lvsl.example.com
              pvs1.example.com
                      peer
lvsl.example.com
              lvs1.example.com
                      peer
3 entries were displayed.
```

Vserver administrator:

```
lvsl.example.com::> vservers peer show
Vserver      Peer      Peer
              Vserver    State
-----
lvsl.example.com
              lvs2.example.com
                      peer
lvsl.example.com
              pvs1.example.com
                      peer
2 entries were displayed.
```

## See Also

`vservers peer show-all`

---

## vserver peer suspend

Suspend a Vserver peer relationship

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer suspend` command suspends the Vserver peer relationship between two Vservers.

### Parameters

**-vserver** <vserver> - Vserver Name

Specifies name of the local Vserver for which you want to suspend the Vserver peer relationship.

**-peer-vserver** <text> - Peer Vserver Name

Specifies name of the peer Vserver for which you want to suspend the Vserver peer relationship.

**[-force [true]]** - Force Suspend

Suspends the Vserver peer relationship even if the remote cluster is not accessible due to, for example, network connectivity issues.

### Examples

The following example illustrates how to suspend the Vserver peer relationship between two Vservers `lvs1.example.com` residing on Cluster1, and `pvs1.example.com` residing on Cluster2.

```
Cluster1::> vserver peer suspend -vserver lvs1.example.com -peer-vserver  
pvs1.example.com
```

### See Also

`vserver peer delete` `vserver peer resume`

---

## vserver peer transition create

Create a new transition peer relationship between a 7-Mode system and a Vserver.

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer transition create` command creates a transition peer relationship between a 7-Mode system and a Vserver.

### Parameters

**-local-vserver** <vserver name> - Local Vserver name

Specifies the name of the local Vserver.

**-src-filer-name** <text> - Source 7-Mode system

Specifies the name of the source 7-Mode system(hostname or IP address).

**[-multi-path-address <text>]** - Additional address for source 7-Mode system

Additional address(hostname or IP address) for the source 7-Mode system.

### Examples

The following example illustrates how to create a transition peer relationship between Vserver vs1.example.com, residing on Cluster1, and a 7-Mode system src1.example.com. We can also specify an additional multipath address src1-e0d.example.com, for load balancing.

```
Cluster1::> vserver peer transition create -vserver vs1.example.com -src-filer-name src1.example.com -multi-path-address src1-e0d.example.com
```

### See Also

`vserver peer transition modify`   `vserver peer transition delete`  
`vserver peer transition show`

---

## vserver peer transition delete

Delete a transition peer relationship.

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer transition delete` command deletes the transition peer relationship.

### Parameters

**-local-vserver** <vserver name> - Local Vserver name

Specifies the name of the local Vserver.

**-src-filer-name** <text> - Source 7-Mode system

Specifies the name of the source 7-Mode system(hostname or IP address).

### Examples

The following example illustrates how to delete the transition peer relationship between a Vserver `lvs1.example.com` residing on `Cluster1`, and source 7-Mode system `src1.example.com`.

```
Cluster1::> vserver peer transition delete -vserver lvs1.example.com -src-filer-name src1.example.com
```

### See Also

`vserver peer transition create`   `vserver peer transition modify`  
`vserver peer transition show`

---

## vserver peer transition modify

Modify a transition peer relationship.

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver peer transition modify` command modifies the multipath address of the transition peer relationship.

### Parameters

**-local-vserver** <vserver name> - Local Vserver name

Specifies the name of the local Vserver.

**-src-filer-name** <text> - Source 7-Mode system

Specifies the name of the source 7-Mode system(hostname or IP address).

**[-multi-path-address** <text>] - Additional address for source 7-Mode system

Additional address(hostname or IP address) for the source 7-Mode system.

### Examples

The following example illustrates how to modify a transition peer relationship's multipath address.

```
Cluster1::> vserver peer transition modify -vserver vs1.example.com -src-filer-name src1.example.com -multi-path-address src1-e0b.example.com
```

### See Also

`vserver peer transition create`   `vserver peer transition delete`

`vserver peer transition show`

---

## vserver peer transition show

Display transition peer relationships.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver peer transition show` command displays the following information about transition peer transition relationships:

- Local Vserver name
- Source 7-Mode system
- Multi-path address

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**local-vserver** <vserver name>] - Local Vserver name

If this parameter is specified, the command displays transition peer information about the specified local Vserver.

[-**src-filer-name** <text>] - Source 7-Mode system

If this parameter is specified, the command displays transition peer information about the specified source 7-Mode system.

[-**multi-path-address** <text>] - Additional address for source 7-Mode system

If this parameter is specified, the command displays information about the specified multipath-address.

### Examples



---

```
Cluster1::> vserver peer transition show
Vserver  Source Filer  Multi Path Address
-----
vs1.example.com
      src1.example.com      src1-e0b.example.com
```

## See Also

vserver peer transition create   vserver peer transition modify  
vserver peer transition delete

---

## vserver security file-directory apply

Apply security descriptors on files and directories defined in a policy to a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory apply` command applies security settings to files and directories defined in a security policy of a Vserver.

Applying a security policy to a Vserver is the last step to creating and applying NTFS ACLs to files or folders. A security policy contains definitions for the security configuration of a file (or folder) or set of files (or, folders). The policy is a container for tasks. A task associates a file/folder path name to the security descriptor that needs to be set on the file/folder. Every task in a policy is uniquely identified by the file/folder path. A policy cannot have duplicate task entries. There can be only one task per path.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

The `vserver security file-directory apply` command is not supported for Vservers with Infinite Volume.

---

## Parameters

**-vserver** <vserver> - Vserver

Specifies the Vserver that contains the path to which the security policy is applied.

**-policy-name** <Security policy name> - Policy Name

Specifies the security policy to apply.

## Examples

The following example applies a security policy named “p1” to Vserver vs0.

```
cluster::> vsserver security file-directory apply -vserver vs0 -  
policy-name p1
```

## vserver security file-directory show

Display file/folder security information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vsserver file-directory show` command displays file/folder security information. The command output depends on the parameter or parameters specified with the command.

The `-vserver` and `-path` parameters are required for this command. If you do not specify any of the optional parameters, the command displays all security information in list format for the specified path.

You can specify the `-fields` parameter to specify which fields of information to display about files and folders security.

You can specify the `-instance` parameter to display all the security information in list format.

The `vsserver security file-directory show` command is not supported for Vservers with Infinite Volume.

## Parameters

{ **[-fields** <fieldname>, ...]

---

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**-vserver** <vserver> - Vserver

Use this required parameter to specify the Vserver that contains the path to the file or folder specified with the required `-path` parameter.

**-path** <text> - File Path

Use this required field to specify the path of the file or folder for which you want to display security information. If the volume name is not specified in the path, the path is relative to the Vserver root volume.

{ **[-volume-name** <volume name>] - Volume Name

If you specify this parameter, the command displays information about file and directory security only for files and directories where the specified path is relative to the specified volume. If this parameter is not specified, the Vserver root volume is taken as default.

| **[-share-name** <Share>] } - Share Name

If you specify this parameter, the command displays information about file and directory security only for files and directories contained where the specified path is relative to the root of the specified share. If this parameter is not specified, the Vserver root volume is taken as default.

**[-lookup-names** {true|false}] - SID to Name Lookups

If set to true the command displays information about file and directory security for files and directories where the information about owner and group are stored as names. If set to false the command displays information about file and directory security for files and directories where the information for owner and group are stored as SIDs.

**[-expand-mask** {true|false}] - Expand Bit Masks

If set to true the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are in expanded bit form. If set to false the command displays information about file and directly security for files and directories where the hexadecimal bit mask entries are in collapsed form.

**[-security-style** {unix|ntfs|mixed|unified}] - Security Style

If you specify this parameter, the command displays information about file and directory security only for files and directories with paths in volumes of the specified security

---

style. The unified security style, which applies only to Infinite Volumes, cannot be applied to file/folder security.

**[-effective-style {unix|ntfs|mixed|unified}]** - Effective Style

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified effective security style on the path. The unified security style, which applies only to Infinite Volumes, cannot be applied to file/folder security.

**[-dos-attributes <Hex Integer>]** - DOS Attributes

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified DOS attributes.

**[-text-dos-attr <TextNoCase>]** - DOS Attributes in Text

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified text DOS attributes.

**[-expanded-dos-attr <TextNoCase>]** - Expanded Dos Attributes

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified extended DOS attributes. This parameter is useful only for files or directories where the `-expand-mask` is set to true.

**[-user-id <user name>]** - Unix User Id

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX user ID.

**[-group-id <group name>]** - Unix Group Id

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX group ID.

**[-mode-bits <Octal Permission>]** - Unix Mode Bits

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX mode bits in Octal form.

**[-text-mode-bits <text>]** - Unix Mode Bits in Text

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX mode bits in text form.

**[-acls <Security acl>, ...]** - ACLs

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified ACLs. The following ACL information can be entered:

- Type of ACL - NTFS or NFSV4
- Control bits in the security descriptors
- Owner - only in case of NTFS security descriptors
- Group - only in case of NTFS security descriptors
- Access Control Entries - discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL

## Examples

The following example displays the security information about the path "/vol4" in Vserver vs1.

```
cluster::> vserver security file-directory show -vserver vs1 -path /
vol4      (vserver security file-directory show)
          Vserver: vs1
          File Path: /vol4
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner:BUILTIN\Administrators
                Group:BUILTIN\Administrators
                DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO
```

The following example displays the security information about the path "/a/b/file.txt" in Vserver vs1.

```
cluster::> vserver security file-directory show -vserver vs1 -
path /a/b/file.txt -volume-name voll
          (vserver security file-directory show)
          Vserver: vs1
          File Path: /voll/a/b/file.txt
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner:BUILTIN\Administrators
                Group:BUILTIN\Administrators
                DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO
```

---

## See Also

vserver file-directory show

---

## vserver security file-directory job show

Display a list of file security jobs

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory job show` command displays information about security file-directory jobs.

To display detailed information about a specific job, run the command with the `-id` parameter.

You can specify additional parameters to select information that matches the values you specify for those parameters. For example, to display information only about security file-directory jobs running on a specific node, run the command with the `-node` parameter.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-inprogress]**

Displays the job ID, the job name, the owning Vserver, and the progress of the security file-directory job.

| **[-jobstate]**

Displays information about each job's state, including the queue state, whether the job was restarted and when the job has completely timed out.

| **[-sched]**

Displays the job ID, the job name, the owning Vserver, and the schedule on which the security file-directory job runs.

| **[-times]**



---

Displays the job ID, the job name, the owning Vserver, the time when the job was last queued, the time when the job was last started, and the time when the job most recently ended.

| **[-type ]**

Displays the job ID, the job name, the job type, and the job category.

| **[-jobuuid ]** (privilege: advanced)

Displays the job ID, the job name, the owning Vserver, and the job UUID.

| **[-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-id <integer>]** - Job ID

Selects the jobs that match the ID or range of IDs that you specify.

**[-vserver <vserver name>]** - Owning Vserver

Selects jobs that are owned by the specified Vserver.

**[-name <text>]** - Name

Selects the jobs that match this parameter value.

**[-description <text>]** - Description

Selects the jobs that match this parameter value.

**[-priority {Low|Medium|High|Exclusive}]** - Priority

Selects the jobs that match this parameter value.

**[-node <nodename>]** - Node

Selects the jobs that match this parameter value.

**[-affinity {Cluster|Node}]** - Affinity

Selects the jobs that match this parameter value.

**[-schedule <job\_schedule>]** - Schedule

Selects the jobs that match this parameter value.

**[-queuetime <MM/DD HH:MM:SS>]** - Queue Time

Selects the jobs that match this parameter value.

**[-starttime <MM/DD HH:MM:SS>]** - Start Time

---

Selects the jobs that match this parameter value.

**[-endtime <MM/DD HH:MM:SS>]** - End Time

Selects the jobs that match this parameter value.

**[-dropdeadtime <MM/DD HH:MM:SS>]** - Drop-dead Time

Selects the jobs that match this parameter value.

**[-restarted {true|false}]** - Restarted?

Selects the jobs that match this parameter value.

**[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}]** - State

Selects the jobs that match this parameter value.

**[-code <integer>]** - Status Code

Selects the jobs that match this parameter value.

**[-completion <text>]** - Completion String

Selects the jobs that match this parameter value.

**[-jobtype <text>]** - Job Type

Selects the jobs that match this parameter value.

**[-category <text>]** - Job Category

Selects the jobs that match this parameter value.

**[-uuid <UUID>]** - UUID

Selects the jobs that match this parameter value.

**[-progress <text>]** - Execution Progress

Selects the jobs that match this parameter value.

**[-username <text>]** - User Name

Selects the jobs that match this parameter value.

**[-process <text>]** - Process

Selects jobs with the specified process number.

## Examples

The following example displays information about the file-directory security job.

---

```
vs1 cluster::>vserver security file-directory apply -policy-name pol -vserver
cluster::>vserver security file-directory job show
      Owning
Job ID Name          Vserver      Node          State
-----
25      Fsecurity Apply    vsim2.3      vsim2.3-01    Success
      Description: File Directory Security Apply Job
```

---

## vserver security file-directory ntfs create

Create an NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs create` command creates an NTFS security descriptor to which you can add access control entries (ACEs) to the discretionary access control list (DACL) and the system access control list (SACL).

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within a namespace. Later, you will associate the security descriptor to a policy task.

You can create NTFS security descriptors for files and folders residing within FlexVol volumes with NTFS security-style or on NTFS security descriptors on mixed security-style volumes.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding a SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create a policy task.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

The `vserver security file-directory ntfs create` command is not supported for Vservers with Infinite Volume.

Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver on which to create the security descriptor.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor you want to create. After you create a security descriptor, you can add SACL and DACL access control entries (ACEs) to it.

Note:

Every newly created security descriptor contains the 4 default DACL ACEs as mentioned below:

Vserver: vserver1				
NTFS Security Descriptor Name: sd1				
	Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----	
folder, sub-folders, files	BUILTIN\Administrators	allow	full-control	this-
	BUILTIN\Users	allow	full-control	this-
	CREATOR OWNER	allow	full-control	this-
	NT AUTHORITY\SYSTEM	allow	full-control	this-
folder, sub-folders, files				

**[-owner** <name or sid>] - Owner of the Security Descriptor

Specifies the owner of the security descriptor. You can specify the owner using either a user name or SID.

The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

---

Note:

If you specify any of the three user name formats for the value of `-owner`, keep in mind that the value for the user name is case insensitive.

**[-group <name or sid>]** - Primary Group of the Owner (privilege: advanced)

Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-group`, keep in mind that the value for the user name is case insensitive.

**[-control-flags-raw <Hex Integer>]** - Raw Control Flags (privilege: advanced)

Specifies the control flags in the security descriptor.

## Examples

The following example creates an NTFS security descriptor named “sd1” on Vserver “vs1” and assigns “DOMAIN\Administrator” as the security descriptor owner.

```
cluster::> vserver security file-directory ntfs create -ntfs-sd sd1
-vserver vs1 -owner DOMAIN\Administrator

cluster::> vserver security file-directory ntfs show -vserver vs1 -
ntfs-sd sd1
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\Administrator
```

---

## vserver security file-directory ntfs delete

Delete an NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs delete` command deletes an NTFS security descriptor. Deleting a security descriptor also deletes all the contained DACL and SACL access control entries (ACEs).

The `vserver security file-directory ntfs delete` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver that is associated with the security descriptor that you want to delete.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor to delete.

### Examples

The following example deletes an NTFS security descriptor named "sd1" on Vserver vs1.

```
cluster::>vserver security file-directory ntfs delete -ntfs-sd sd1 -  
vserver vs1
```

## vserver security file-directory ntfs modify

Modify an NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

---

The `vserver security file-directory ntfs modify` command modifies an NTFS security descriptor. You can change the `-owner`, `-group` and `-control-flags-raw` of the security descriptor with this command.

The `vserver security file-directory ntfs modify` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor that you want to modify.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that you want to modify.

**[-owner** <name or sid>] - Owner of the Security Descriptor

Specifies the owner of the security descriptor. You can specify the owner using either the user name or SID.

The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-owner`, keep in mind that the value for the user name is case insensitive.

**[-group** <name or sid>] - Primary Group of the Owner (privilege: advanced)

Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID



- 
- Domain\user-name
  - user-name@Domain
  - user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-group`, keep in mind that the value for the user name is case insensitive.

**[-control-flags-raw <Hex Integer>]** - Raw Control Flags (privilege: advanced)

Specifies the control flags in the security descriptor to be modified.

## Examples

The following example modifies the owner of an NTFS security descriptor named "sd2" on Vserver vs1.

```
cluster::>vserver security file-directory ntfs modify -ntfs-sd
sd2 -vserver vs1 -owner domain\administrator

cluster::>vserver security file-directory ntfs show -vserver vs1
-ntfs-sd sd2
Vserver: vs1
Security Descriptor Name: sd2
Owner of the Security Descriptor: DOMAIN\Administrator
```

---

## vserver security file-directory ntfs show

Display an NTFS security descriptors

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver file-directory ntfs show` command displays information about the security descriptor. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays all information about all security descriptors defined on the cluster.

You can specify the `-fields` parameter to specify which fields of information to display about security descriptors.

You can specify the `-instance` parameter to display all the information about security descriptors in list format.

The `vserver security file-directory ntfs show` command is not supported for Vservers with Infinite Volume.

### Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver** <vserver>] - Vserver

If you specify this parameter, the command displays information only about the security descriptors associated with the Vserver that you specify.

**[-ntfs-sd** <ntfs sd name>] - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the security descriptors that you specify.

**[-owner** <name or sid>] - Owner of the Security Descriptor

---

If you specify this parameter, the command displays information only about the security descriptors owned by the specified user name or SID.

**[-group <name or sid>]** - Primary Group of the Owner (privilege: advanced)

If you specify this parameter, the command displays information only about the security descriptors associated with the owner group.

**[-control-flags-raw <Hex Integer>]** - Raw Control Flags (privilege: advanced)

If you specify this parameter, the command displays information only about the security descriptors associated with the control flags.

## Examples

The following example displays information about an NTFS security descriptor named “sd2” on Vserver vs1.

```
ntfs-sd sd2      cluster::> vs1 security file-directory ntfs show -vs1 -
                  Vserver: vs1
                  Security Descriptor Name: sd2
                  Owner of the Security Descriptor: DOMAIN\Administrator
```

## See Also

vs1 file-directory ntfs show

---

## vserver security file-directory ntfs dacl add

Add a DACL entry to NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs dacl add` command adds access control entries (ACEs) into a security descriptor's discretionary access control list (DACL).

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

Adding a DACL entry to the security descriptor is the second step in configuring and applying ACLs to a file or folder. Before you can add a DACL entry to a security descriptor, you must first create the security descriptor.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

---

The `vserver security file-directory ntfs dacl add` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor to which you want to add a discretionary access control entry (discretionary ACE).

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor to which you want to add a discretionary access control entry.

**-access-type** {deny|allow} - Allow or Deny

Specifies whether the discretionary access control entry is an allow or deny type of access control.

**-account** <name or sid> - Account Name or SID

Specifies the account on which to apply the discretionary access control entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-account`, keep in mind that the value for the user name is case insensitive.

{ **-rights** {no-access|full-control|modify|read-and-execute|read|write}} - DACL ACE's Access Rights

Specifies the right that you want to add for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- 
- no-access
  - full-control
  - modify
  - read-and-execute
  - read
  - write

| [**-advanced-rights** <Advanced access right>, ...] - DACL ACE's Advanced Access Rights

Specifies the advanced rights that you want to add for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| [**-rights-raw** <Hex Integer>] } - DACL ACE's Raw Access Rights (privilege: advanced)

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `rights-raw` parameter is mutually exclusive with the `-advanced-`

---

`rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: `0xA10F` or `0xb3ff` etc.

**[`-apply-to` {this-folder|sub-folders|files}, ...]** - Apply DACL Entry

Specifies where to apply the discretionary access control entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

## Examples

The following example adds a DACL entry to the security descriptor named "sd1" on Vserver "vs1" for the "DOMAIN\Administrator" account.

```
cluster::>vserver security file-directory ntfs dacl add -ntfs-  
sd sd1 -access-type deny -account DOMAIN\Administrator -rights full-control -  
apply-to this-folder -vserver vs1
```

```
cluster::>vserver security file-directory ntfs dacl show -  
vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\administrator
```

```
          Vserver: vs1  
Security Descriptor Name: sd1  
          Allow or Deny: deny  
          Account Name or SID: DOMAIN\Administrator  
          Access Rights: full-control  
Advanced Access Rights: -  
          Apply To: this-folder  
          Access Rights: full-control
```

---

## vserver security file-directory ntfs dacl modify

Modify an NTFS security descriptor DACL entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs dacl modify` command modifies parameters in an existing discretionary access control (DACL) entry.

You can unambiguously define which DACL entry to modify by specifying the following four parameters in the modify command:

- Vserver associated with the security descriptor that contains the DACL entry
- Name of the security descriptor that contains the DACL entry
- Whether the DACL is an allow or deny type of DACL entry
- The account name or SID to which the DACL is applied

You can modify the following parameters:

- `-right,-advanced-rights ,-rights-raw`
- `-apply-to`

The `vserver security file-directory ntfs dacl modify` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor containing the discretionary access control entry whose parameters you want to modify.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the discretionary access control entry that you want to modify.

**-access-type** {deny|allow} - Allow or Deny



---

Specifies whether the discretionary access control entry that you want to modify is an allow or deny type of access control.

**-account** <name or sid> - Account Name or SID

Specifies the account associated with the discretionary access control entry you want to modify. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of -account, keep in mind that the value for the user name is case insensitive.

{ **[-rights** {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

Specifies the right that you want to add for the account specified in the -account parameter. The -rights parameter is mutually exclusive with the -advanced-rights and -rights-raw parameter. If you specify the -rights parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

| **[-advanced-rights** <Advanced access right>, ...] - Advanced Access Rights

Specifies the advanced rights that you want to add for the account specified in the -account parameter. The -advanced-rights parameter is mutually exclusive with the -rights and -rights-raw parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

---

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| **[-rights-raw <Hex Integer>] }** - Raw Access Rights (privilege: advanced)

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: 0xA10F or 0xb3ff etc.

**[-apply-to {this-folder|sub-folders|files}, ...]** - Apply DACL Entry

Specifies where to apply the discretionary access control entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

## Examples

---

The following example modifies the `-right` and `-apply-to` parameters in the DACL entry associated to the security descriptor named “sd2” on Vserver vs1 for the "BUILTIN\Administrators" account.

```
cluster::>vserver security file-directory ntfs dacl modify -ntfs-  
sd sd2 -access-type allow -account BUILTIN\Administrators -vserver vs1 -rights  
modify -apply-to this-folder,sub-folders  
  
cluster::>vserver security file-directory ntfs dacl show -vserver vs1  
-ntfs-sd sd2 -account BUILTIN\Administrators -instance  
  
Vserver: vs1  
Security Descriptor Name: sd2  
Allow or Deny: allow  
Account Name or SID: BUILTIN\Administrators  
Access Rights: modify  
Advanced Access Rights: -  
Apply To: this-folder, sub-folders  
Access Rights: modify
```

---

## vserver security file-directory ntfs dacl remove

Remove a DACL entry from NTFS security descriptor.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs dacl remove` command removes a discretionary access control entry from a security descriptor.

You can unambiguously define which DACL entry to remove by specifying the following four parameters in the command:

- Vserver associated with the security descriptor that contains the DACL entry
- Name of the security descriptor that contains the DACL entry
- Whether the DACL is an allow or deny type of DACL entry
- The account name or SID to which the DACL is applied

The `vserver security file-directory ntfs dacl remove` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor from which you want to remove a discretionary access control entry.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the discretionary access control entry that you want to remove.

**-access-type** {deny|allow} - Allow or Deny

Specifies whether the discretionary access control entry you want to remove is an allow or deny of access control.

**-account** <name or sid> - Account Name or SID

Specifies the account name or SID associated with the discretionary access control entry that you want to remove.

---

## Examples

The following example removes a DACL entry from the security descriptor named “sd2” with “allow” access type for the “BUILTIN\Administrators” account on Vserver vs1.

```
cluster::>vserver security file-directory ntfs dacl remove -ntfs-sd
sd2 -access-type allow -account BUILTIN\Administrators -vserver vs1
```

## vserver security file-directory ntfs dacl show

Display NTFS security descriptor DACL entries

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs dacl show` command displays information about all the discretionary access control entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all DACL entries:

- Vserver name
- Security descriptor
- List of DACL entries

You can specify the `-fields` parameter to specify which fields of information to display about DACL entries.

You can specify the `-instance` parameter to display all information about DACL entries in a list format.

The `vserver security file-directory ntfs dacl show` command is not supported for Vservers with Infinite Volume.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| [-**instance** ] }

---

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**`[-vserver <vserver>]`** - Vserver

If you specify this parameter, the command displays information only about discretionary access control entries associated with the specified Vserver.

**`[-ntfs-sd <ntfs sd name>]`** - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the discretionary access control entries for the security descriptor that you specify.

**`[-access-type {deny|allow}]`** - Allow or Deny

If you specify this parameter, the command displays information only about the discretionary access control entries with the access type that you specify.

**`[-account <name or sid>]`** - Account Name or SID

If you specify this parameter, the command displays information only about the discretionary access control entries associated with the account name or SID that you specify. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-account`, keep in mind that the value for the user name is case insensitive.

**`[-rights {no-access|full-control|modify|read-and-execute|read|write}]`** - Access Rights

If you specify this parameter, the command displays information only about the discretionary access control entries with the user right that you specify. Only one value can be specified.

You can specify one of the following rights values:

- no-access
- full-control
- modify

- 
- read-and-execute
  - read
  - write

**[-advanced-rights <Advanced access right>, ...]** - Advanced Access Rights

If you specify this parameter, the command displays information only about the discretionary access control entries with the advanced user rights that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

**[-rights-raw <Hex Integer>]** - Raw Access Rights (privilege: advanced)

If you specify this parameter, the command displays information only about the discretionary access control entries with the advanced user rights that you specify. This value for this parameter is mutually exclusive with any other rights values. Specify the value as a hexadecimal integer, for example: 0xA10F or 0xb3ff etc.

**[-apply-to {this-folder|sub-folders|files}, ...]** - Apply DACL Entry

If you specify this parameter, the command displays information only about the discretionary access control entries with the -applied-to value or values that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

**[-readable-access-rights <TextNoCase>] - Access Rights**

If you specify this parameter, the command displays information only the discretionary access control entries with the readable access rights that you specify.

**Examples**

The following example shows information about a DACL entry.

```
cluster::>vserver security file-directory ntfs dacl show
Vserver: vs1
NTFS Security Descriptor Name: sd2
    Account Name      Access  Access
    -----      Type   Rights
folders, files      BUILTIN\Users    allow    full-control    this-folder, sub-
folders, files      CREATOR OWNER    allow    full-control    this-folder, sub-
folders, files      NT AUTHORITY\SYSTEM
                                allow    full-control    this-folder, sub-
3 entries were displayed.
```



---

## vserver security file-directory ntfs sacl add

Add a SACL entry to NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs sacl add` command adds system access control list entries (ACEs) into a security descriptor's system access control list (SACL).

If the security descriptor contains a SACL that has existing security ACEs, the command adds the new security ACE to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new security ACE to it.

Adding a SACL entry to the security descriptor is the second step in configuring and applying security ACLs to a file or folder. Before you can add a SACL entry to a security descriptor, you must first create the security descriptor.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACL and SACL entries to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

---

The `vserver security file-directory ntfs sac1 add` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor to which you want to add a system access control list entry.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor to which you want to add a system access control list entry.

**-access-type** {failure|success} - Failure or Success

Specifies whether the system access control list entry that you want to add is a failure or success access audit type.

**-account** <name or sid> - Account Name or SID

Specifies the account on which to apply the system access control list entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-account`, keep in mind that the value for the user name is case insensitive.

{ **-rights** {no-access|full-control|modify|read-and-execute|read|write}} - Access Rights

Specifies the right that you want to add for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access

- 
- full-control
  - modify
  - read-and-execute
  - read
  - write

| [**-advanced-rights** <Advanced access right>, ...] - Advanced Access Rights

Specifies the advanced rights that you want to add for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| [**-rights-raw** <Hex Integer>] } - Raw Access Rights (privilege: advanced)

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: 0xA10F or 0xb3ff etc.

---

**[-apply-to {this-folder|sub-folders|files}, ...]** - Apply SACL To

Specifies where to apply the system access control list entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

## Examples

The following example adds a SACL entry to the security descriptor named “sd1” on Vserver vs1.

```
cluster::>vserver security file-directory ntfs sac1 add -ntfs-sd
sd1 -access-type failure -account DOMAIN\Administrator -rights full-control -
apply-to this-folder -vserver vs1
cluster::>vserver security file-directory ntfs sac1 show -vserver
vs1 -ntfs-sd sd1 -access-type deny -account DOMAIN\Administrator
```

```

                                Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\Administrator
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

---

## vserver security file-directory ntfs sacl modify

Modify an NTFS security descriptor SACL entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs sacl modify` command modifies parameters in an existing system access control list entry.

You can unambiguously define which SACL entry to modify by specifying the following four parameters in the modify command:

- Vserver associated with the security descriptor that contains the SACL entry
- Name of the security descriptor that contains the SACL entry
- Whether the SACL is a success or failure type of SACL entry
- The account name or SID to which the SACL is applied

You can modify the following parameters:

- `-rights,-advanced-rights,-rights-raw`
- `-apply-to`

The `vserver security file-directory ntfs sacl modify` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor containing the system access control list entry whose fields you want to modify.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the system access control list entry that you want to modify.

**-access-type** {failure|success} - Failure or Success

---

Specifies whether the system access control list entry that you want to modify is a failure or success access audit type.

**-account** <name or sid> - Account Name or SID

Specifies the account on which to apply the system access control list entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-account`, keep in mind that the value for the user name is case insensitive.

**{ [-rights {no-access|full-control|modify|read-and-execute|read|write}]** - Access Rights

Specifies the right that you want to add for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

**| [-advanced-rights <Advanced access right>, ...]** - Advanced Access Rights

Specifies the advanced rights that you want to add for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

---

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| **[-rights-raw <Hex Integer>] }** - Raw Access Rights (privilege: advanced)

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: 0xA10F or 0xb3ff etc.

**[-apply-to {this-folder|sub-folders|files}, ...]** - Apply SACL To

Specifies where to apply the system access control list entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

## Examples

The following example modifies the rights and `-apply-to` fields in the SACL entry.

---

```
cluster::>vserver security file-directory ntfs sac1 modify -ntfs-sd
sd2 -access-type success -account BUILTIN\Administrators -vserver vs1 -rights
modify -apply-to this-folder,sub-folders

cluster::>vserver security file-directory ntfs sac1 show -vserver vs1
-ntfs-sd sd2 -account BUILTIN\Administrators -instance

Vserver: vs1
Security Descriptor Name: sd2
Access type for Specified Access Rights: success
Account Name or SID: BUILTIN\Administrators
Access Rights: modify
Advanced Access Rights: -
Apply To: this-folder, sub-folders
Access Rights: modify
```



---

## vserver security file-directory ntfs sac1 remove

Remove a SACL entry from NTFS security descriptor

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs sac1 remove` command removes a system access control list entry from a security descriptor.

You can unambiguously define which SACL entry to remove by specifying the following four parameters in the command:

- Vserver associated with the security descriptor that contains the SACL entry
- Name of the security descriptor that contains the SACL entry
- Whether the SACL is a success or failure type of SACL entry
- The account name or SID to which the SACL is applied

The `vserver security file-directory ntfs sac1 remove` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security descriptor from which you want to remove the system access control list entry.

**-ntfs-sd** <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the system access control list entry that you want to remove.

**-access-type** {failure|success} - Failure or Success

Specifies whether the system access control list entry that you want to remove is a failure or success access audit type.

**-account** <name or sid> - Account Name or SID

Specifies the account name or SID associated with the system access control list entry that you want to remove.

---

## Examples

The following example removes a SACL entry named “sd2” on Vserver vs1 with an access type of “success” associated with the “BUILTIN\Administrators” account.

```
cluster::>vserver security file-directory ntfs sac1 remove -ntfs-sd
sd2 -access-type success -account BUILTIN\Administrators -vserver vs1
```

## vserver security file-directory ntfs sac1 show

Display NTFS security descriptor SACL entries

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory ntfs sac1 show` command displays information about all the system access control list entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all SACL entries:

- Vserver name
- Security descriptor
- List of SACL entries

You can specify the `-fields` parameter to specify which fields of information to display about SACL entries.

You can specify the `-instance` parameter to display all information about SACL entries in a list format.

The `vserver security file-directory ntfs sac1 show` command is not supported for Vservers with Infinite Volume.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| [-**instance** ] }

---

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**`[-vserver <vserver>]`** - Vserver

If you specify this parameter, the command displays information only about system access control list entries associated with the specified Vserver.

**`[-ntfs-sd <ntfs sd name>]`** - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the system access control list entries for the security descriptor that you specify.

**`[-access-type {failure|success}]`** - Failure or Success

If you specify this parameter, the command displays information only about the system access control list entries with the access type that you specify.

**`[-account <name or sid>]`** - Account Name or SID

If you specify this parameter, the command displays information only about the system access control list entries associated with the account name or SID that you specify. You can use any of the following formats when specifying the value for this parameter:

- SID
- Domain\user-name
- user-name@Domain
- user-name@FQDN

Note:

If you specify any of the three user name formats for the value of `-account`, keep in mind that the value for the user name is case insensitive.

**`[-rights {no-access|full-control|modify|read-and-execute|read|write}]`** - Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the user right that you specify. The value for this parameter is mutually exclusive with any other rights values. Only one value can be specified.

You can specify one of the following rights values:

- no-access
- full-control
- modify

- 
- read-and-execute
  - read
  - write

**[-advanced-rights <Advanced access right>, ...]** - Advanced Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the advanced user rights that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following advanced rights values:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

**[-rights-raw <Hex Integer>]** - Raw Access Rights (privilege: advanced)

If you specify this parameter, the command displays information only about the system access control list entries with the advanced user rights that you specify. This value for this parameter is mutually exclusive with any other rights values. Specify the value as a hexadecimal integer, for example: 0xA10F or 0xb3ff etc.

**[-apply-to {this-folder|sub-folders|files}, ...]** - Apply SACL To

---

If you specify this parameter, the command displays information only about the system access control list entries with the `-applied-to` value or values that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- `this-folder`
- `sub-folder`
- `files`

**`[-readable-access-rights <TextNoCase>]` - Access Rights**

If you specify this parameter, the command displays information only about the system access control list entries with the readable access rights that you specify.

**Examples**

The following example shows a SACL entry.

```
cluster::>vserver security file-directory sacl show
(vserver security file-directory ntfs sacl show)

Vserver: vs1
NTFS Security Descriptor Name: sdl

  Account Name      Access  Access      Apply To
      Type          Rights
-----
domain\user        success full-control  this-folder, sub-
folders, files
```

---

## vserver security file-directory policy create

Create a file security policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory policy create` command creates a security policy for a Vserver. A policy acts as a container for various tasks where each task is a single entry that can be applied to a file/folder.

Creating a security policy is the third step in configuring and applying security ACLs to a file or folder. You will later add tasks to the security policy.

Note:

You cannot modify a security policy. If you want to apply a policy with the same settings to a different Vserver, you must create a new policy with the same configuration and apply it to the desired Vserver.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLS and SACLs to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding SACLs to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

---

The `vserver security file-directory policy create` command is not supported for Vservers with Infinite Volume.

**Parameters**

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver on which to create the security policy.

**-policy-name** <Security policy name> - Policy Name

Specifies the name of the security policy.

**Examples**

The following example creates a security policy named “policy1” on Vserver vs1.

```
cluster::>vserver security file-directory policy create -policy-name
policy1 -vserver vs1
cluster::>vserver security file-directory policy show

Vserver      Policy Name
-----
vs1          policy1
```

---

## vserver security file-directory policy delete

Delete a file security policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory policy delete` command deletes a security policy from a Vserver.

The `vserver security file-directory policy delete` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the name of the Vserver associated with the security policy that you want to delete.

**-policy-name** <Security policy name> - Policy Name

Specifies the name of the security policy you want to delete.

### Examples

The following example deletes a security policy named “policy1” from Vserver vs1.

```
cluster::>vserver security file-directory policy delete -policy-name  
policy1 -vserver vs1
```

## vserver security file-directory policy show

Display file security policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description



---

The `vserver security file-directory policy show` command displays information about all security policies in the Vserver. The command output depends on the parameter or parameters specified with the command.

You can specify the `-fields` parameter to specify which fields of information to display about security policies.

You can specify the `-instance` parameter to display information for all security policies in a list format.

The `vserver security file-directory policy show` command is not supported for Vservers with Infinite Volume.

## Parameters

{ **[-fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver>]** - Vserver

If you specify this parameter, the command displays information only about security policies associated with the specified Vserver.

**[-policy-name <Security policy name>]** - Policy Name

If you specify this parameter, the command displays information only about the security policy you specify.

## Examples

The following example displays information about the security policies on the cluster.

```
cluster::>vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
vs1          policy2
2 entries were displayed.
```

---

## vserver security file-directory policy task add

Add a policy task

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory policy task add` command adds a single task entry to a security policy. A task refers to a single operation that can be done by a security policy to a file/folder.

Before you create a security policy task you must first create a security policy and a security descriptor. You should also add DACL entries and SACL entries (if desired) to the security descriptor before you create the security policy task.

Note:

You can add DACL and SACL entries to the security descriptor after you have associated it to a security policy task.

Creating a policy task is the fourth step in configuring and applying ACLs to a file or folder. When you create the policy task, you associate a security descriptor to it. You also associate the task to a security policy.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLS and SACLs to the NTFS security descriptor.

Note:

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding SACLs to the Security Descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.

- Create policy tasks.

---

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

- Apply a policy to the associated Vserver.

The `vserver security file-directory policy task add` command is not supported for Vservers with Infinite Volume.

## Parameters

**-vserver** <vserver> - Vserver

Specifies the Vserver associated with the security policy to which you want to add a task.

**-policy-name** <Security policy name> - Policy Name

Specifies the name of the security policy into which you want to add the task.

**-path** <text> - Path

Specifies the path of the file/folder on which to apply the security descriptor associated with this task.

**[-security-type {ntfs|nfsv4}]** - Security Type of the File

Specifies whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is “ntfs”.

Note:

The nfsv4 security descriptor type is not supported in this release. If you specify this optional parameter, you must enter ntfs for the -security-type value.

**[-ntfs-mode {propagate|ignore|replace}]** - Propagation Mode

Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and/or folders contained within a parent folder inherit access control and audit information from the parent folder.

You can specify one of the three parameter values that correspond to three types of propagation modes:

- propagate - propagate inheritable permissions to all subfolders and files

- replace - replace existing permissions on all subfolders and files with inheritable permissions
- ignore - do not allow permissions on this file or folder to be replaced

**[-ntfs-sd <ntfs sd name>]** - NTFS Security Descriptor Name

Specifies the name of security descriptor to apply to the path specified in the `-path` parameter.

**[-index-num <integer>]** - Position

Specifies the index number of a task. Tasks are applied in order. A task with a larger index value is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.

The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.

Note:

If you specify an index number that is already assigned to an existing task, index number will be auto arranged to highest index number in the table.

## Examples

The following example adds a security policy task entry to the policy named “policy1” on Vserver vs1.

```
cluster::>vserver security file-directory policy task add -vserver
vs1 -policy-name policy1 -path / -security-type ntfs -ntfs-mode propagate -ntfs-
sd sd -index-num 1
cluster::>vserver security file-directory policy task show

Vserver: vs1
Policy: policy1
  Index  File/Folder  Security  NTFS  NTFS Security
  -----  -----  Type      Mode  Descriptor Name
  1         /          ntfs      propagate  sd
```

---

## vserver security file-directory policy task modify

Modify a policy task

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory policy task modify` command modifies a task entry in a security policy.

You can unambiguously define which task to modify by specifying the following three parameters in the modify command:

- Vserver associated with the task
- Name of the security policy that contains the task
- Name of the path to which the task is applied

You can modify the following parameters:

- `-ntfs-mode`
- `-ntfs-sd`
- `-index-num`

Note:

The only security type supported in this Data ONTAP release is “ntfs”; therefore, you cannot modify the `-security-type` parameter.

The `vserver security file-directory policy task modify` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the Vserver associated with the security policy that contains the task you want to modify.

**-policy-name** <Security policy name> - Policy Name

---

Specifies the name of the security policy that contains the task you want to modify.

**-path** <text> - Path

Specifies the path of the file/folder associated with the task that you want to modify.

**[-security-type {ntfs|nfsv4}]** - Security Type

Specifies whether the security descriptor in the task that you want to modify should be an NTFS security descriptor type or an NFSv4 security descriptor type. Default value is ntfs.

Note:

The nfsv4 security descriptor type is not supported in this release. If you specify this optional parameter, you must enter ntfs for the -security-type value.

**[-ntfs-mode {propagate|ignore|replace}]** - NTFS Propagation Mode

Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and/or folders contained within a parent folder inherit access control and audit information from the parent folder.

You can specify one of the three parameter values that correspond to three types of propagation modes:

- propagate - propagate inheritable permissions to all subfolders and files
- replace - replace existing permissions on all subfolders and files with inheritable permissions
- ignore - do not allow permissions on this file or folder to be replaced

**[-ntfs-sd <ntfs sd name>]** - NTFS Security Descriptor Name

Specifies the name of security descriptor to apply to the path specified in the -path parameter.

**[-index-num <integer>]** - Position

Specifies the index number of a task. Tasks are applied in order. A task with a larger index value is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.

The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.

Note:

---

If you specify an index number that is already assigned to an existing task, the command fails when you attempt to create a duplicate entry.

**Examples**

The following example modifies the ntfs mode, index, and ntfs-sd parameters in the security policy task entry.

```
cluster:>vserver security file-directory policy task modify -
vserver vs1 -policy-name policy1 -path / -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd -index-num 1
cluster:>vserver security file-directory policy task show -vserver
vs1 -policy-name policy1

Vserver: vs1
Policy: policy1
Index      File/Folder      Security      NTFS      NTFS Security
-----      Path      Type      Mode      Descriptor Name
1            /      ntfs      propagate  sd
```

---

## vserver security file-directory policy task remove

Remove a policy task

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security file-directory policy task remove` command removes a task entry from a security policy.

The `vserver security file-directory policy task remove` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver> - Vserver

Specifies the Vserver associated with the security policy that contains the task you want to remove.

**-policy-name** <Security policy name> - Policy Name

Specifies the name of the security policy that contains the task you want to remove.

**-path** <text> - Path

Specifies the path of the file/folder associated with the task that you want to remove.

### Examples

The following example removes a security policy task entry.

```
cluster::>vserver security file-directory policy task remove -  
vserver vs1 -policy-name policy1 -path /
```

## vserver security file-directory policy task show

Display policy tasks

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.



---

## Description

The `vserver security file-directory policy task show` command displays information about all the task entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all task entries:

- Vserver name
- Policy name
- Task entries

The `vserver security file-directory policy task show` command is not supported for Vservers with Infinite Volume.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver>]** - Vserver

If you specify this parameter, the command displays information only tasks associated with the specified Vserver.

**[-policy-name <Security policy name>]** - Policy Name

If you specify this parameter, the command displays information only about tasks associated with the specified security policy.

**[-path <text>]** - Path

If you specify this parameter, the command displays information only about tasks applied to the specified path.

**[-security-type {ntfs|nfsv4}]** - Security Type

If you specify this parameter, the command displays information only about tasks associated with the specified security type.

Note:

The nfsv4 security descriptor type is not supported in this release.

**[-ntfs-mode {propagate|ignore|replace}] - NTFS Propagation Mode**

If you specify this parameter, the command displays information only about tasks configured with the NTFS propagation mode that you specify.

**[-ntfs-sd <ntfs sd name>] - NTFS Security Descriptor Name**

If you specify this parameter, the command displays information only about the policy tasks associated with the NTFS security descriptor that you specify.

**[-index-num <integer>] - Position**

If you specify this parameter, the command displays information only about tasks assigned the index number that you specify.

**Examples**

The following example displays policy task entries for a policy named “policy1” on Vserver vs1.

```
cluster::>yserver security file-directory policy task show -vserver
vs1 -policy-name policy1
Vserver: vs1
Policy: policy1
  Index  File/Folder Path  Security Type  NTFS Mode  NTFS Security Descriptor Name
  ----  -
  1      /                    ntfs        propagate  sd
```

---

## vserver security trace filter create

Create a security trace entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security trace filter create` command creates a security trace filter entry. This feature is currently supported for CIFS only and not supported for NFS.

The `vserver security trace filter create` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver on which the permission trace is applied.

**-index** <integer> - Filter Index

This specifies the index number you want to assign to the trace filter. A maximum of 10 entries can be created. The allowed values for this parameter are 1 through 10.

**[-client-ip** <IP Address>] - Client IP Address to Match

This specifies the IP Address from which the user is accessing the Vserver.

**[-path** <TextNoCase>] - Path

This specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share for CIFS or the root of the volume for NFS that the client is accessing, or the value can be a part of the path that the client is accessing. Use NFS style directory separators in the path value.

{ **[-windows-name** <TextNoCase>] - Windows User Name

This specifies the Windows user name to trace. You can use any of the following formats when specifying the value for this parameter:

- user\_name
- domain\user\_name

| **[-unix-name** <TextNoCase>] } - UNIX User Name

---

This specifies the Unix user name to trace.

**[-trace-allow {yes|no}]** - Trace Allow Events

Security tracing can trace deny events and allow events. Deny event tracing is always ON by default. Allow events can optionally be traced. If set to yes, this option allows tracing of allow events. If set to no, allow events are not traced.

**[-enabled {enabled|disabled}]** - Filter Enabled

This specifies whether to enable or disable the filter. Filters are enabled by default.

**[-time-enabled <integer>]** - Minutes Filter is Enabled

This specifies a timeout for this filter, after which it is disabled.

## Examples

The following example creates a security trace filter.

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1 -time-enabled 120 -client-ip 10.72.205.207
```

The following examples create filters that include the `-path` option. If the client is accessing a file with the path `\\server\sharename\dir1\dir2\dir3\file.txt`, a complete path starting from the root of the share or a partial path can be given as shown:

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1 -path /dir1/dir2/dir3/file.txt
cluster1::> vserver security trace filter create -vserver vs0 -index 1 -path dir3/file.txt
```

## vserver security trace filter delete

Delete a security trace entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security trace filter delete` command deletes a security trace filter entry. This feature is currently supported for CIFS only and not supported for NFS.

The `vserver security trace filter delete` command is not supported for Vservers with Infinite Volume.

### Parameters

---

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver on which the tracing filter entry that you want to delete is applied.

**-index** <integer> - Filter Index

This specifies the index number for the filter that you want to delete. You can display a list of the filter index numbers by using the `vserver security trace filter show` command.

## Examples

The following example deletes a security trace filter.

```
cluster1::> vserver security trace filter delete -vserver vs0 -index 1
```

## See Also

`vserver security trace filter show`

---

## vserver security trace filter modify

Modify a security trace entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security trace filter modify` command modifies a security trace filter entry. This feature is currently supported for CIFS only and not supported for NFS.

The `vserver security trace filter modify` command is not supported for Vservers with Infinite Volume.

### Parameters

**-vserver** <vserver name> - Vserver

This specifies the name of the Vserver on which the permission trace is applied.

**-index** <integer> - Filter Index

This specifies the index number for the filter. A maximum of 10 entries can be created. The allowed values for this parameter are 1 through 10.

**[-client-ip** <IP Address>] - Client IP Address to Match

This specifies the IP Address from which the user is accessing the Vserver.

**[-path** <TextNoCase>] - Path

This specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share for CIFS or the root of the volume for NFS that the client is accessing, or the value can be a part of the path that the client is accessing. Use NFS style directory separators in the path value.

**{ [-windows-name** <TextNoCase>] - Windows User Name

This specifies the Windows user name to trace. You can use any of the following formats when specifying the value for this parameter:

- `user_name`
- `domain\user_name`

---

| **[-unix-name <TextNoCase>]** } - UNIX User Name

This specifies the Unix user name to trace.

**[-trace-allow {yes|no}]** - Trace Allow Events

Security tracing can trace deny events and allow events. Deny event tracing is always ON by default. Allow events can optionally be traced. If set to yes, this option allows tracing of allow events. If set to no, allow events are not traced.

**[-enabled {enabled|disabled}]** - Filter Enabled

This specifies whether to enable or disable the filter. Filters are enabled by default.

**[-time-enabled <integer>]** - Minutes Filter is Enabled

This specifies a timeout for this filter, after which it is disabled.

## Examples

The following example modifies a security trace filter.

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1 -time-enabled 120 -client-ip 10.72.205.207
```

The following examples modify filters that include the `-path` option. If the client is accessing a file with the path `\\server\sharename\dir1\dir2\dir3\file.txt`, a complete path starting from the root of the share or a partial path can be given as shown:

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1 -path /dir1/dir2/dir3/file.txt
cluster1::> vserver security trace filter modify -vserver vs0 -index 1 -path dir3/file.txt
```

## vserver security trace filter show

Display a security trace entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver security trace filter show` command displays information about security trace filter entries. This feature is currently supported for CIFS only and not supported for NFS.

The `vserver security trace filter show` command is not supported for Vservers with Infinite Volume.

---

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified Vserver.

**[-index <integer>]** - Filter Index

If you specify this parameter, the command displays permission tracing information only for filters with the specified filter index number.

**[-client-ip <IP Address>]** - Client IP Address to Match

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified client IP address.

**[-path <TextNoCase>]** - Path

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified path.

**[-windows-name <TextNoCase>]** - Windows User Name

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified Windows user name.

**[-unix-name <TextNoCase>]** - UNIX User Name

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified UNIX user name.

**[-trace-allow {yes|no}]** - Trace Allow Events

If you specify this parameter, the command displays information only about events that either trace or do not trace allow events, depending on the value provided.

**[-enabled {enabled|disabled}]** - Filter Enabled



---

If you specify this parameter, the command displays information only about filters that either are enabled or disabled, depending on the value provided.

**[-time-enabled <integer>]** - Minutes Filter is Enabled

If you specify this parameter, the command displays information only about filters that are disabled after the specified minutes.

## Examples

The following example displays security trace filters for Vserver vserver1.

```
clus::> vserver security trace filter show
Vserver  Index      Client-IP      Path      Trace-Allow  Windows-Name
-----  -
vserver1  1      -              -          no           domain\user
vserver1  2      192.168.2.3    -          yes          -
vserver1  3      -              /dir1/dir2/file  no           domain\
                                     administrator
```

3 entries were displayed.

---

## vserver security trace trace-result delete

Delete security trace results

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Delete the specified security tracing event record.

The `vserver security trace trace-result delete` command is not supported for Vservers with Infinite Volume.

### Parameters

**-node** {<nodename>|local} - Node

This specifies the cluster node on which the permission tracing event that you want to delete occurred.

**-vserver** <vserver> - Vserver

This specifies the Vserver on which the permission tracing event that you want to delete occurred.

**-seqnum** <integer> - Sequence Number

This specifies the sequence number of the log entry to be deleted.

### Examples

The following example deletes the security trace result record for the Vserver `vserver_1` on node `Node_1` whose sequence number is 999.

```
cluster1::> vserver security trace trace-result delete -vserver vserver_1 -node  
Node_1 -seqnum 999
```

## vserver security trace trace-result show

Display security trace results

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver security trace trace-result show` command displays the list of security trace event records stored on the cluster. These records are generated in response to security trace filters that are created using the `vserver security trace filter create` command. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all the security trace events generated since the filter was enabled:

- Vserver name
- Cluster node name
- Security trace filter index number
- User name
- Security style
- Path
- Reason

You can specify additional parameters to display only information that match those parameters. For example, to display information about events that occurred for the user "guest", run the command with `-user-name` parameter set to guest.

The `vserver security trace trace-result show` command is not supported for Vservers with Infinite Volume.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify this parameter, the command only displays the fields that you specify.

| **[-instance ]** }

If you specify this parameter, the command displays detailed information about all security trace events.

**[-node {<nodename>|local}]** - Node

If you specify this parameter, the command displays information only about security trace events on the specified node.

**[-vserver <vserver>]** - Vserver

---

If you specify this parameter, the command displays information only about security trace events on the specified Vserver.

**[-seqnum <integer>]** - Sequence Number

If you specify this parameter, the command displays information only about the security trace events with this sequence number.

**[-keytime <Date>]** - Time

If you specify this parameter, the command displays information only about security trace events that occurred at the specified time.

**[-index <integer>]** - Index of the Filter

If you specify this parameter, the command displays information only about security trace events that occurred as a result of the filter corresponding to the specified filter index number.

**[-client-ip <IP Address>]** - Client IP Address

If you specify this parameter, the command displays information only about security trace events that occurred as a result of file access from the specified client IP address.

**[-path <TextNoCase>]** - Path of the File Being Accessed

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file accesses to the specified path.

**[-user-name <TextNoCase>]** - Windows or Unix User Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file accesses by the specified user.

**[-security-style <security style>]** - Effective Security Style On File

If you specify this parameter, the command displays information only about the security trace events that occurred on file systems with the specified security style. The allowed values for security style are the following:

- SECURITY\_NONE - Security not Set
- SECURITY\_UNIX\_MODEBITS - UNIX and UNIX permissions
- SECURITY\_UNIX\_ACL - UNIX and NFSv4 ACL
- SECURITY\_UNIX\_SD - UNIX and NT ACL
- SECURITY\_MIXED\_MODEBITS - MIXED and UNIX permissions
- SECURITY\_MIXED\_ACL - MIXED and NFSv4 ACL
- SECURITY\_MIXED\_SD - MIXED and NT ACL

- 
- SECURITY\_NTFS\_MODEBITS - NTFS and UNIX permissions
  - SECURITY\_NTFS\_ACL - NTFS and NT ACL
  - SECURITY\_NTFS\_SD - NTFS and NT ACL
  - SECURITY\_UNIX - UNIX
  - SECURITY\_MIXED - MIXED
  - SECURITY\_NTFS - NTFS
  - SECURITY\_MODEBITS - UNIX permissions
  - SECURITY\_ACL - ACL
  - SECURITY\_SD - SD

**[-result <TextNoCase>]** - Result of Security Checks

If you specify this parameter, the command displays information only about the security trace events that have the specified result. Access to a file or a directory can be 'allowed' or 'denied'. Output from this command displays the result as a combination of the reason for allowing or denying access and the location where access is either allowed or denied.

The following are the reasons why an access can be allowed:

- Access is allowed because the operation is trusted and no security is configured
- Access is allowed because the user has UNIX root privileges
- Access is allowed because the user has UNIX owner privileges
- Access is allowed because UNIX implicit permission grants requested access
- Access is allowed because the CIFS user is owner
- Access is allowed because the user has take ownership privilege
- Access is allowed because there is no CIFS ACL
- Access is allowed because CIFS implicit permission grants requested access
- Access is allowed because the security descriptor is corrupted and the user is a member of the Administrators group
- Access is allowed because the ACL is corrupted and the user is a member of the Administrators group
- Access is allowed because the user has UNIX permissions
- Access is allowed because explicit ACE grants requested access

- 
- Access is allowed because the user has audit privileges
  - Access is allowed because the user has superuser credentials
  - Access is allowed because inherited ACE grants requested access

The following are the reasons why an access can be denied:

- Access is denied by UNIX permissions
- Access is denied by an explicit ACE
- Access is denied. The requested permissions are not granted by the ACE
- Access is denied. The security descriptor is corrupted
- Access is denied. The ACL is corrupted
- Access is denied. The sticky bit is set on the parent directory and the user is not the owner of file or parent directory
- Access is denied. The owner can be changed only by root
- Access is denied. The UNIX permissions/uid/gid/NFSv4 ACL can be changed only by owner or root
- Access is denied. The GID can be set by owner to a member of its legal group list only if 'Owner can chown' is not set
- Access is denied. The file or the directory has readonly bit set
- Access is denied. There is no audit privilege
- Access is denied. Enforce DOS bits blocks the access
- Access is denied. Hidden attribute is set
- Access is denied by an inherited ACE

The command or the location at which access was denied or allowed are as follows:

- while traversing the directory.
- while truncating the file.
- while creating the directory.
- while creating the file.
- while checking parent's mode bits during delete.
- while deleting the child.
- while checking for child-delete access on the parent.

- 
- while reading security descriptor.
  - while accessing the link.
  - while creating the directory.
  - while creating or writing the file.
  - while opening existing file or directory.
  - while setting the attributes.
  - while traversing the directory.
  - while reading the file.
  - while reading the directory.
  - while deleting the target during rename.
  - while deleting the child during rename.
  - while writing data in the parent during rename.
  - while adding a directory during rename.
  - while adding a file during rename.
  - while updating the target directory during rename.
  - while setting attributes.
  - while writing to the file.
  - while extending the coral file.
  - while creating the vdisk file.
  - while checking for stale locks before open.
  - while deleting a file or a directory.
  - while truncating a hidden file.

## Examples

The following example displays information about security trace records:

```
clus-01::> vserver security trace trace-result show
Vserver: vserver_1
```

Node	Index	Filter Details	Reason
clus-01	1	User: cifs1\administrator	Access is allowed because CIFS implicit permission grants requested access while opening existing file or directory.

---

```
clus-01          1      Security Style: MIXED
                    and NT ACL
                    Path: /stk/bit
                    User: cifs1\
                    administrator
                    Access is allowed because
                    explicit ACE grants
                    requested access while
                    opening existing file
                    or directory.

                    Security Style: MIXED
                    and NT ACL
                    Path: /stk/bit
```

2 entries were displayed.

The following example displays information about security trace records for path /stk/bit/set:

```
clus-01::> vserver security trace trace-result show -path /stk/bit/set
Vserver: vserver_1
```

Node	Index	Filter Details	Reason
clus-01	1	User: cifs1\administrator	Access is allowed because the user has UNIX root privileges while opening existing file or directory.
clus-01	1	Security Style: MIXED and UNIX permissions Path: /stk/bit/set User: cifs1\administrator	Access is denied. The requested permissions are not granted by the ACE while checking for child-delete access on the parent.
clus-01	1	Security Style: MIXED and NT ACL Path: /stk/bit/set User: cifs1\administrator	Access is allowed because the CIFS user is owner. Access is denied by an explicit ACE while setting the attributes.
		Security Style: MIXED and NT ACL Path: /stk/bit/set	

3 entries were displayed.

## See Also

vserver security trace filter create



---

## vserver services dns create

Create a new DNS table entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services dns create` command creates new DNS server mappings. DNS servers provide remote connection information, such as IP addresses, based on domain and system names.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver on which to create the new DNS server mapping.

**-domains** <text>, ... - Domains

Use this parameter to specify the domains of the Vserver. Separate multiple domains with commas.

**[-name-servers** <IP Address>, ...] - Name Servers

Use this parameter to specify the IP addresses of the DNS servers that provide name service for the domains in this DNS server mapping. Separate multiple addresses with commas.

**-state** {enabled|disabled} - Enable/Disable DNS

Use this parameter with the value `enabled` to specify that the DNS server mapping is active when it is created. Use this parameter with the value `disabled` to specify that the DNS server mapping is not active.

**[-timeout** <integer>] - Timeout (secs)

Use this parameter to specify a timeout value (in seconds) for queries to the name servers. The default value is 2 seconds.

**[-attempts** <integer>] - Maximum Attempts

Use this parameter to specify the number of attempts the Vserver should make when querying the DNS name servers. The default value is 1 attempt.

---

## Examples

This example creates a new DNS server mapping for the Vserver vs0 in the domain example.com, specifying that 192.168.0.16 and 192.168.0.24 are the name servers for this domain.

```
cluster1::> vserver services dns create -vserver vs0 -domains example.com -name-servers 192.168.0.16,192.168.0.24
```

## vserver services dns delete

Remove a DNS table entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services dns delete` command removes the DNS server mapping from a Vserver.

Deleting a DNS server mapping removes it permanently. If you delete a DNS server mapping, commands or jobs that do not use IP addresses do not succeed. To disable a DNS server mapping without deleting it, use the `vserver services dns modify` command with the `-state disabled` parameter.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver whose DNS server mapping is deleted.

## Examples

This example removes the DNS server mapping from the Vserver node1.

```
cluster1::> vserver services dns delete -vserver vs0
```

### See Also

`vserver services dns modify`

---

## vserver services dns modify

Change a DNS table entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `vserver services dns modify` command to modify an existing DNS server mapping.

Use the `-state disabled` parameter to disable a DNS server mapping without deleting it. To permanently remove a mapping, use the `vserver services dns delete` command.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver whose DNS mapping is modified.

**[-domains** <text>, ...] - Domains

Use this parameter to specify a domain for the Vserver.

**[-name-servers** <IP Address>, ...] - Name Servers

Use this parameter to specify the IP addresses of the DNS name servers for this Vserver.

**[-state** {enabled|disabled}] - Enable/Disable DNS

Use this parameter with the value `enabled` to specify that the DNS server mapping is active. Use this parameter with the value `disabled` to specify that the DNS server mapping is not active.

**[-timeout** <integer>] - Timeout (secs)

Use this parameter to specify a timeout value (in seconds) for queries to the DNS servers.

**[-attempts** <integer>] - Maximum Attempts

Use this parameter to specify the number of times to attempt queries to the DNS servers.

---

## Examples

This example modifies the DNS server mapping for the domain example.com on the Vserver vs0, specifying that 10.0.0.1 and 10.0.0.2 are the name servers for this domain.

```
cluster1::> vsriver services dns modify -vsriver vs0 -domains example.com -name-servers 10.0.0.1,10.0.0.2
```

The following example disables the DNS mapping for example.com on a Vserver named vs1:

```
cluster1::> vsriver services dns modify -vsriver vs1 -domains example.com -state disabled
```

## See Also

`vsriver services dns delete`

---

## vserver services dns show

Display DNS configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services dns show` command displays information about DNS server mappings. DNS servers provide remote connection information, such as IP addresses, based on domain and system names.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

Use this parameter to display information only about the DNS server mapping of the Vservers you specify.

[-**domains** <text>, ...] - Domains

Use this parameter to display information only about the DNS server mappings for Vservers in the domains you specify.

[-**name-servers** <IP Address>, ...] - Name Servers

Use this parameter to display information only about DNS server mappings that use the DNS name servers you specify.

[-**state** {enabled|disabled}] - Enable/Disable DNS

Use this parameter with the value `enabled` to display information only about the DNS server mappings that are active. Use this parameter with the value `disabled` to display information only about the DNS server mappings that are not active.

**[-timeout <integer>]** - Timeout (secs)

Use this parameter to display information only about DNS server mappings that have the timeout value you specify.

**[-attempts <integer>]** - Maximum Attempts

Use this parameter to display information only about DNS server mappings that make the maximum number of attempts you specify.

### Examples

The following example shows typical output from the command. Note that cluster1 uses different name servers for example.com.

```
cluster1::> vserver services dns show
```

Vserver	State	Domains	Name Servers
node1	enabled	example.com	10.0.0.1, 10.0.0.2
node2	enabled	example.com, example2.com	10.0.0.1, 10.0.0.2
cluster1	enabled	example.com, example2.com	192.168.0.1, 192.168.0.2

---

## vserver services dns hosts create

Create a new host table entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `vserver services dns hosts create` command to create new DNS host table entries. These entries map hostnames to IP addresses.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver on which the host table entry will be created.

**-address** <IP Address> - IP Address

Use this parameter to specify the IP address of the new host table entry.

**-hostname** <text> - Canonical Hostname

Use this parameter to specify the full hostname for the new host table entry.

**[-aliases** <text>, ...] - Aliases

Use this parameter to specify any aliases to include in the new host table entry. Separate multiple aliases with commas.

### Examples

This example creates a new DNS host table entry for 10.0.0.17 on the node `node1`, with the hostname `test.example.com` and the alias `test`.

```
cluster1::> vserver services dns hosts create -vserver node1 -address 10.0.0.17 -hostname test.example.com -aliases test
```

## vserver services dns hosts delete

Remove a host table entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

Use the `vserver services dns hosts delete` command to delete DNS host table entries.

## Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver whose host table entry will be deleted.

**-address** <IP Address> - IP Address

Use this parameter to specify the IP address of the host table entry to delete.

## Examples

This example removes the DNS host table entry of 10.0.0.15 from the host table of the node `node1`.

```
cluster1::> vserver services dns hosts delete -vserver node1 -address 10.0.0.16
1 entry was deleted.
```

## vserver services dns hosts modify

Modify hostname or aliases

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

Use the `vserver services dns hosts modify` command to modify existing DNS host table entries.

## Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver whose host table will be modified.

**-address** <IP Address> - IP Address

Use this parameter to specify the IP address of the host table entry to modify.

**[-hostname <text>]** - Canonical Hostname

Use this parameter to specify a full hostname for the host table entry.



---

**[-aliases <text>, ...]** - Aliases

Use this parameter to specify alternate hostnames for the host table entry.

## Examples

This example changes the host table of node `node1` so that the hostname stored in the host table entry for 10.0.0.57 is `pgh.example.com`.

```
cluster1::> vservice services dns hosts modify -node node1 -address 10.0.0.57 -
hostname pgh.example.com
1 entry was modified.
```

This example changes the host table of node `node1` to store the name `loghost` as an alternate hostname for IP address 10.0.0.5.

```
cluster1::> vservice services dns hosts modify -node node1 -address 10.0.0.5 -
aliases loghost
1 entry was modified.
```

## vservice services dns hosts show

Display IP address to hostname mappings

**Availability:** This command is available to *cluster* and *Vservice* administrators at the *admin* privilege level.

## Description

Use the `vservice services dns hosts show` command to display Domain Name System (DNS) host table entries. These entries map hostnames to IP addresses. Entries may also include alternate hostnames, known as aliases. Host table entries enable you to refer to other Internet hosts by a memorable name instead of by a numeric IP address. This host table is similar to the `/etc/hosts` file found on most UNIX style systems.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

---

**[-vserver <vserver name>]** - Vserver

Use this parameter to display information only about host table entries on the Vservers you specify.

**[-address <IP Address>]** - IP Address

Use this parameter to display information only about host table entries that match the IP addresses you specify.

**[-hostname <text>]** - Canonical Hostname

Use this parameter to display information only about host table entries that match the hostnames you specify.

**[-aliases <text>, ...]** - Aliases

Use this parameter to display information only about host table entries that include the alternate hostnames you specify.

## Examples

The following example shows a typical host table.

```
cluster::> vserver services dns hosts show
Vserver      Address      Hostname      Aliases
-----
node1        10.0.0.10    mail.example.com
node1        10.0.0.15    ftp.example.com ftp
node1        10.0.0.16    www.example.com www
node2        10.0.0.10    mail.example.com
node2        10.0.0.15    ftp.example.com ftp
node2        10.0.0.16    www.example.com www
node2        10.0.0.17    test.example.com
7 entries were displayed.
```

---

## vserver services kerberos-realm create

Create a Kerberos realm configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver services kerberos-realm create` command creates a Kerberos realm configuration.

### Parameters

**-configname** <text> - Configuration Name

This parameter specifies the name of the Kerberos realm configuration that you want to create.

**-realm** <text> - Kerberos Realm

This parameter specifies the name of the Kerberos realm for the configuration.

**-kdc-vendor** <Kerberos Key Distribution Center (KDC) Vendor> - KDC Vendor

This optional parameter specifies the KDC vendor. Specify Microsoft if you are using a Microsoft Active Directory server; specify Other if you are using a UNIX server.

**-kdc-ip** <IP Address> - KDC IP Address

This optional parameter specifies the IP address of the Kerberos Distribution Center (KDC) server.

**[-kdc-port <integer>]** - KDC Port

This optional parameter specifies the port number of the KDC server. The default setting is 88.

**[-clock-skew <integer>]** - Clock Skew

This optional parameter specifies how many seconds of clock skew between the clients and the server are permitted. The default setting is 300 seconds.

**[-adserver-name <text>]** - Active Directory Server Name

This optional parameter specifies the name of an Active Directory server for the configuration. Use this parameter only if you specified the value of `-kdc-vendor` parameter as Microsoft.

---

**[-adserver-ip <IP Address>]** - Active Directory Server IP Address

This optional parameter specifies the IP address of an Active Directory server for the configuration. Use this parameter only if you specified the value of the `-kdc-vendor` parameter as Microsoft.

**[-comment <text>]** - Comment

This optional parameter specifies a comment for the Kerberos realm configuration.

**[-adminserver-ip <IP Address>]** - Admin Server IP Address

This optional parameter specifies the IP address of the administrative server. Use this parameter only if you specified the value of `-kdc-vendor` parameter as Other. The default setting for this parameter is the KDC server's IP address as specified by the `-kdc-ip` parameter.

**[-adminserver-port <integer>]** - Admin Server Port

This optional parameter specifies the port number of the administrative server. The default setting is 749. Use this parameter only if you specified the value of `-kdc-vendor` parameter as Other.

**[-passwordserver-ip <IP Address>]** - Password Server IP Address

This optional parameter specifies the IP address of the password server. Use this parameter only if you specified the value of `-kdc-vendor` parameter as Other. The default setting for this parameter is the KDC server's IP address as specified by the `-kdc-ip` parameter.

**[-passwordserver-port <integer>]** - Password Server Port

This optional parameter specifies the port number of the password server. The default setting is 464. Use this parameter only if you specified the value of `-kdc-vendor` parameter as Other.

## Examples

The following example creates a Kerberos realm configuration named AUTH. The configuration uses the Kerberos realm SEC.EXAMPLE.COM. The permitted clock skew is 15 seconds. The KDC's IP address is 192.0.2.170 and its port is 88. The KDC vendor is Other (for a UNIX KDC). The administrative server's IP address is 192.0.2.170 and its port is 749. The password server's IP address is 192.0.2.170 and its port is 464.

```
cluster1::> vserver services kerberos-realm create -configname AUTH
-realm SEC.EXAMPLE.COM -clock-skew 15 -kdc-ip 192.0.2.170 -kdc-port 88
-kdc-vendor Other -adminserver-ip 192.0.2.170 -adminserver-port 749
-passwordserver-ip 192.0.2.170 -passwordserver-port 464
```

---

## vserver services kerberos-realm delete

Delete a Kerberos realm configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver services kerberos-realm delete` command deletes a Kerberos realm configuration from the system.

### Parameters

**-configname** <text> - Configuration Name

This specifies the name of the Kerberos realm configuration that you want to delete.

### Examples

The following example deletes a Kerberos realm configuration named SECURITY:

```
cluster1::> vserver services kerberos-realm delete -configname SECURITY
```

## vserver services kerberos-realm modify

Modify a Kerberos realm configuration

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver services kerberos-realm modify` command modifies one or more attributes of a Kerberos realm configuration.

### Parameters

**-configname** <text> - Configuration Name

This parameter specifies the name of the Kerberos realm configuration that you want to modify.

**[-realm <text>]** - Kerberos Realm

---

This optional parameter specifies the name of a Kerberos realm for the configuration.

**[-kdc-vendor <Kerberos Key Distribution Center (KDC) Vendor>]** - KDC Vendor

This optional parameter specifies the KDC vendor. Specify Microsoft if you are using a Microsoft Active Directory server; specify Other if you are using a UNIX server.

**[-kdc-ip <IP Address>]** - KDC IP Address

This optional parameter specifies the IP address of the Kerberos Distribution Center (KDC) server.

**[-kdc-port <integer>]** - KDC Port

This optional parameter specifies the port number of the KDC server. The default setting at the time of creation is 88.

**[-clock-skew <integer>]** - Clock Skew

This optional parameter specifies how many seconds of clock-skew between server and the clients are permitted. The default setting at the time of creation is 300 seconds.

**[-adserver-name <text>]** - Active Directory Server Name

This optional parameter specifies the name of an Active Directory server for the configuration. Use this parameter if you specified the value of `-kdc-vendor` parameter as Microsoft.

**[-adserver-ip <IP Address>]** - Active Directory Server IP Address

This optional parameter specifies the IP address of an Active Directory server for the configuration. Use this parameter if you specified the value of the `-kdc-vendor` parameter as Microsoft.

**[-comment <text>]** - Comment

This optional parameter specifies a comment for the Kerberos realm configuration.

**[-adminserver-ip <IP Address>]** - Admin Server IP Address

This optional parameter specifies the IP address of the administrative server. Use this parameter if you specified the value of `-kdc-vendor` parameter as Other.

**[-adminserver-port <integer>]** - Admin Server Port

This optional parameter specifies the port number of the administrative server. The default setting at the time of creation is 749. Use this parameter if you specified the value of the `-kdc-vendor` parameter as Other.

**[-passwordserver-ip <IP Address>]** - Password Server IP Address

---

This optional parameter specifies the IP address of the password server. Use this parameter if you specified the value of `-kdc-vendor` parameter as `Other`.

**`[-passwordserver-port <integer>]`** - Password Server Port

This optional parameter specifies the port number of the password server. The default setting at the time of creation is 464. Use this parameter only if you specified the value of `-kdc-vendor` parameter as `Other`.

## Examples

The following example modifies the Kerberos realm configuration named `AUTH` to use a Microsoft KDC server with the IP address `192.0.2.170` and an Active Directory server named `AUTH.SEC.EXAMPLE.COM` with the IP address `192.0.2.170`:

```
cluster1::> vservice services kerberos-realm modify -configname AUTH -adserver-  
name AUTH.SEC.EXAMPLE.COM  
-adserver-ip 192.0.2.170 -kdc-ip 192.0.2.170 -kdc-vendor Microsoft
```

---

## vserver services kerberos-realm show

Display Kerberos realm configurations

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

The `vserver services kerberos-realm show` command displays information about Kerberos realm configurations. The command output depends on the parameters specified with the command. If you do not specify any parameters, the command displays the following information about all Kerberos realm configurations:

- Configuration name
- Kerberos realm name
- Active Directory server name
- Kerberos Distribution Center (KDC) vendor
- KDC IP address

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**configname** <text>] - Configuration Name

If you specify this parameter, the command displays information only about the Kerberos realm configurations that match the specified name.

[-**realm** <text>] - Kerberos Realm

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified Kerberos realm.

[-**kdc-vendor** <Kerberos Key Distribution Center (KDC) Vendor>] - KDC Vendor



---

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified KDC vendor.

**[-kdc-ip <IP Address>]** - KDC IP Address

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified KDC IP address.

**[-kdc-port <integer>]** - KDC Port

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified KDC port number.

**[-clock-skew <integer>]** - Clock Skew

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified clock skew.

**[-adserver-name <text>]** - Active Directory Server Name

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the Active Directory server that has the specified name.

**[-adserver-ip <IP Address>]** - Active Directory Server IP Address

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the Active Directory server that has the specified IP address.

**[-comment <text>]** - Comment

If you specify this parameter, the command displays information only about the Kerberos realm configurations that match the specified comment text.

**[-adminserver-ip <IP Address>]** - Admin Server IP Address

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified administrative-server IP address.

**[-adminserver-port <integer>]** - Admin Server Port

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified administrative-server port number.

**[-passwordserver-ip <IP Address>]** - Password Server IP Address

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified password-server IP address.

**[-passwordserver-port <integer>]** - Password Server Port

---

If you specify this parameter, the command displays information only about the Kerberos realm configurations that use the specified password-server port number.

### Examples

The following example displays information about all Kerberos realm configurations:

```
cluster1::> vserver services kerberos-realm show
Configuration Kerberos Active Directory KDC Vendor KDC
Name Realm Server Other IP Address
DEVkrb NFSDEV.MIT.REALM - Other 172.17.16.65
```

---

## vserver services ldap create

Create an LDAP configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap create` command associates an LDAP client configuration with a Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver with which you want to associate the LDAP client configuration.

**-client-config** <text> - LDAP Client Configuration

This parameter specifies the name of the LDAP client configuration, defined under `vserver services ldap client`, that you want to associate with the Vserver.

**-client-enabled** {true|false} - LDAP Client Enabled

This parameter specifies whether the Vserver can use the LDAP configuration.

Note:

You must also include the 'ldap' method in the Vserver's `-ns-switch` and/or `-nm-switch` parameters before a Vserver uses an enabled LDAP configuration.

### Examples

The following example associates the LDAP client configuration "corp" with the Vserver "vs1":

```
cluster1::> vserver services ldap create -vserver vs1 -client-config corp
```

### See Also

`vserver services ldap client`

---

## vserver services ldap delete

Delete an LDAP configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap delete` command removes the LDAP configuration, which is an LDAP client configuration's association with a Vserver.

Note:

Make sure that you remove 'ldap' from the Vserver's `-ns-switch` and `-nm-switch` parameters and test connectivity before deleting a working LDAP configuration.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver from which you want to disassociate the LDAP client configuration.

### Examples

The following example disassociates the current LDAP client configuration from Vserver "vs1".

```
cluster1::> vserver services ldap delete -vserver vs1
```

## vserver services ldap modify

Modify an LDAP configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap modify` command modifies an LDAP client configuration's association with a Vserver.

---

Note:

Make sure that you remove 'ldap' from the Vserver's `-ns-switch` and `-nm-switch` configurations and test connectivity before disabling a working LDAP configuration.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver with which you want to associate the LDAP client configuration.

**[-client-config** <text>] - LDAP Client Configuration

This parameter specifies the name of the LDAP client configuration, defined under `vserver services ldap client`, that you want to associate with the Vserver.

**[-client-enabled** {true|false}] - LDAP Client Enabled

This parameter specifies whether the Vserver can use the LDAP configuration.

Note:

You must also include the 'ldap' method in the Vserver's `-ns-switch` and/or `-nm-switch` parameters before a Vserver uses an enabled LDAP configuration.

## Examples

The following example modifies the LDAP client configuration used by Vserver "vs1" to "corpnew":

```
cluster1::> vserver services ldap modify -vserver vs1 -client-config corpnew
```

## See Also

`vserver services ldap client`

---

## vserver services ldap show

Display LDAP configurations

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap show` command displays information about LDAP configurations.

### Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use '`-fields ?`' to display the fields to specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-**vserver** <vserver name>] - Vserver

If you specify this parameter, the command displays information about the LDAP configuration on the specified Vserver.

[-**client-config** <text>] - LDAP Client Configuration

If you specify this parameter, the command displays information about LDAP configurations using the specified client.

[-**client-enabled** {true|false}] - LDAP Client Enabled

If you specify this parameter, the command displays information about LDAP configurations with the matching client state.

### Examples

The following example shows the LDAP configuration for Vserver "vs1":

```
cluster1::> vserver services ldap show -vserver vs1
      Client      Client
Vserver Configuration Enabled
-----
vs1         corp         true
```

---

## vserver services ldap client create

Create an LDAP client configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap client create` command creates an LDAP client configuration. A client configuration is associated with a Vserver using the `vserver services ldap` commands.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which configuration is created.

**-client-config** <text> - Client Configuration Name

This parameter specifies the name that you would like to use to refer to the new LDAP client configuration.

{ **-servers** <IP Address>, ... - LDAP Server List

This parameter specifies the list of LDAP servers used when making LDAP connections using this client configuration. If you specify this parameter, you cannot specify the `-ad-domain`, `-preferred-ad-servers` or `-bind-as-cifs-server` parameters.

| **-ad-domain** <TextNoCase> - Active Directory Domain

This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This assumes that the Active Directory schema has been extended to act as a NIS replacement. If you use this parameter, you cannot specify the `-servers` parameter. However, you can specify a list of preferred servers using the `-preferred-ad-servers` parameter.

[**-preferred-ad-servers** <IP Address>, ...] - Preferred Active Directory Servers

This parameter specifies a list of LDAP servers that are preferred over those that are discovered in the domain specified in the `-ad-domain` parameter.

[**-bind-as-cifs-server** {true|false}] } - Bind Using the Vserver's CIFS Credentials

---

This parameter specifies whether or not LDAP binds made using this client configuration use the Vserver's CIFS server credentials. If you do not specify this parameter, the default is `false`.

**-schema <text>** - Schema Template

This parameter specifies the name of the schema template the Vserver uses when making LDAP queries. You can view and modify the templates using the `vserver services ldap client schema` commands.

**[-port <integer>]** - LDAP Server Port

This parameter specifies the port that the LDAP client uses to connect to LDAP servers. If you do not specify this parameter, the default is port 389.

**[-query-timeout <integer>]** - Query Timeout (sec)

This parameter specifies the amount of time (in seconds) that the LDAP client waits for a query to complete. If you do not specify this parameter, the default is 3 seconds.

**[-min-bind-level {anonymous|simple|sas}]** - Minimum Bind Authentication Level

This parameter specifies the lowest acceptable level of security the LDAP client uses to bind to an LDAP server. If you do not specify this parameter, the default is an `anonymous` bind.

**[-bind-dn <ldap\_dn>]** - Bind DN (User)

This parameter specifies the user that binds to the LDAP servers. For Active Directory servers, specify the user in the account (`DOMAIN\user`) or principal (`user@domain.com`) form. Otherwise, specify the user in distinguished name (`CN=user,DC=domain,DC=com`) form. This parameter is ignored if `-bind-as-cifs-server` is set.

**[-base-dn <ldap\_dn>]** - Base DN

This parameter specifies the default base DN for all searches, including user, group, and netgroup searches. For example, "`DC=example,DC=com`". If you do not specify this parameter, the default is the root, specified by an empty ( " " ) set.

**[-base-scope {base|onelevel|subtree}]** - Base Search Scope

This parameter specifies the default search scope for LDAP queries. Specify `base` to search just the named entry, `onelevel` to search entries immediately below the DN, or `subtree` to search the entire subtree below the DN. If you do not specify this parameter, the default is `subtree` scope.

**[-user-dn <ldap\_dn>]** - User DN (privilege: advanced)

This parameter specifies the user DN, which overrides the base DN for user lookups.



---

**[-user-scope {base|onelevel|subtree}]** - User Search Scope (privilege: advanced)

This parameter specifies the user search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

**[-group-dn <ldap\_dn>]** - Group DN (privilege: advanced)

This parameter specifies the group DN, which overrides the base DN for group lookups.

**[-group-scope {base|onelevel|subtree}]** - Group Search Scope (privilege: advanced)

This parameter specifies the group search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

**[-netgroup-dn <ldap\_dn>]** - Netgroup DN (privilege: advanced)

This parameter specifies the netgroup DN, which overrides the base DN netgroup lookups.

**[-netgroup-scope {base|onelevel|subtree}]** - Netgroup Search Scope (privilege: advanced)

This parameter specifies the netgroup search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

## Examples

The following example creates an LDAP client configuration named `corp` that makes anonymous binds to 172.160.0.100 and 172.16.0.101 for vserver `vs1`:

```
cluster1:> vserver services ldap client create -vserver vs1 -client-config corp -servers 172.160.0.100,172.16.0.101
```

The following example creates an LDAP client configuration named `corp` that makes binds to 172.160.0.100 and 172.16.0.101 for vserver `vs1` for bind-dn `diag`:

```
cluster1:> vserver services ldap client create -vserver vs1 -client-config corp -servers 172.160.0.100,172.16.0.101 -bind-dn diag
Please enter password:
Confirm password:
```

## See Also

`vserver services ldap client schema` `vserver services ldap`

---

## vserver services ldap client delete

Delete an LDAP client configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap client delete` command deletes an LDAP client configuration. A Vserver administrator can only delete configurations owned by the Vserver.

### Parameters

**[-vserver <vserver name>]** - Vserver

This parameter specifies the name of the Vserver which owns the LDAP client you want to delete.

**-client-config <text>** - Client Configuration Name

This parameter specifies the name of the LDAP client configuration you want to delete.

### Examples

The following example deletes an LDAP client configuration named `corp` owned by Vserver `vs1`:

```
cluster1::> vserver services ldap client delete -vserver vs1 -client-config corp
```

## vserver services ldap client modify-bind-password

Modify Bind Password of an LDAP client configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap client modify-bind-password` command modifies bind-password of a given LDAP client configuration.

---

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver which owns the LDAP client you want to modify.

**-client-config** <text> - Client Configuration Name

This parameter specifies the name of the LDAP client configuration.

## Examples

The following example modifies the password for a given LDAP client configuration

```
cluster1::> vserver services ldap client modify-bind-password -client-  
config corp  
Please enter password:  
Confirm password:
```

## vserver services ldap client modify

Modify an LDAP client configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver services ldap client modify` command modifies an LDAP client configuration. A Vserver administrator can modify only configurations owned by the Vserver.

## Parameters

**[-vserver** <vserver name>] - Vserver

This parameter specifies the name of the Vserver which owns the LDAP client you want to modify.

**-client-config** <text> - Client Configuration Name

This parameter specifies the name of the LDAP client configuration.

{ **[-servers** <IP Address>, ...] - LDAP Server List

---

This parameter specifies the list of LDAP servers used when making LDAP connections using this client configuration. If you specify this parameter, you cannot specify the `-ad-domain`, `-preferred-ad-servers` or `-bind-as-cifs-server` parameters.

| **[-ad-domain <TextNoCase>]** - Active Directory Domain

This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This assumes that the Active Directory schema has been extended to act as a NIS replacement. If you use this parameter, you cannot specify the `-servers` parameter. However, you can specify a list of preferred servers using the `-preferred-ad-servers` parameter.

**[-preferred-ad-servers <IP Address>, ...]** - Preferred Active Directory Servers

This parameter specifies a list of LDAP servers that are preferred over those that are discovered in the domain specified in the `-ad-domain` parameter.

**[-bind-as-cifs-server {true|false}] }** - Bind Using the Vserver's CIFS Credentials

This parameter specifies whether or not LDAP binds made using this client configuration use the Vserver's CIFS server credentials. If you do not specify this parameter, the default is `false`.

**[-schema <text>]** - Schema Template

This parameter specifies the name of the schema template the Vserver uses when making LDAP queries. You can view and modify the templates using the `vserver services ldap client schema` commands.

**[-port <integer>]** - LDAP Server Port

This parameter specifies the port that the LDAP client uses to connect to LDAP servers. If you do not specify this parameter, the default is port 389.

**[-query-timeout <integer>]** - Query Timeout (sec)

This parameter specifies the amount of time (in seconds) that the LDAP client waits for a query to complete. If you do not specify this parameter, the default is 3 seconds.

**[-min-bind-level {anonymous|simple|sas}]** - Minimum Bind Authentication Level

This parameter specifies the lowest acceptable level of security the LDAP client uses to bind to an LDAP server. If you do not specify this parameter, the default is an `anonymous` bind.

**[-bind-dn <ldap\_dn>]** - Bind DN (User)

This parameter specifies the user that binds to the LDAP servers. For Active Directory servers, specify the user in the account (`DOMAIN\user`) or principal (`user@domain.com`) form. Otherwise, specify the user in distinguished name

---

(CN=user,DC=domain,DC=com) form. This parameter is ignored if `-bind-as-cifs-server` is set.

**[-base-dn <ldap\_dn>]** - Base DN

This parameter specifies the default base DN for all searches, including user, group, and netgroup searches. For example, "DC=example,DC=com". If you do not specify this parameter, the default is the root, specified by an empty ( " " ) set.

**[-base-scope {base|onelevel|subtree}]** - Base Search Scope

This parameter specifies the default search scope for LDAP queries. Specify `base` to search just the named entry, `onelevel` to search entries immediately below the DN, or `subtree` to search the entire subtree below the DN. If you do not specify this parameter, the default is `subtree` scope.

**[-user-dn <ldap\_dn>]** - User DN (privilege: advanced)

This parameter specifies the user DN, which overrides the base DN for user lookups.

**[-user-scope {base|onelevel|subtree}]** - User Search Scope (privilege: advanced)

This parameter specifies the user search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

**[-group-dn <ldap\_dn>]** - Group DN (privilege: advanced)

This parameter specifies the group DN, which overrides the base DN for group lookups.

**[-group-scope {base|onelevel|subtree}]** - Group Search Scope (privilege: advanced)

This parameter specifies the group search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

**[-netgroup-dn <ldap\_dn>]** - Netgroup DN (privilege: advanced)

This parameter specifies the netgroup DN, which overrides the base DN netgroup lookups.

**[-netgroup-scope {base|onelevel|subtree}]** - Netgroup Search Scope (privilege: advanced)

This parameter specifies the netgroup search scope. If you do not specify a value for this parameter, the value of the `-base-scope` parameter is used.

## Examples

The following example modifies an existing LDAP client configuration named `corp` owned by Vserver `vs1` to require simple binds using the `administrator@example.com` account:

```
cluster1::> vsserver services ldap client modify -client-config corp -vserver vs1  
-bind-dn administrator@example.com
```

---

`-min-bind-level simple`

## See Also

`vserver services ldap client schema`

---

## vserver services ldap client show

Display LDAP client configurations

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap client show` command displays information about LDAP client configurations which a Vserver can be associated with. An LDAP client configuration created by a Vserver's administrator or by the cluster administrator for the Vserver is owned by the Vserver. A cluster-wide LDAP client configuration is created by a cluster administrator by specifying the admin Vserver's name as a value to the `-vserver` parameter. In addition to its owned LDAP client configurations, a Vserver can be associated with such cluster-wide LDAP client configurations.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays all LDAP client configurations that can be associated with the specified Vserver.

**[-client-config <text>]** - Client Configuration Name

If you specify this parameter, the command displays information about the LDAP client configuration you specify.

**[-servers <IP Address>, ...]** - LDAP Server List

If you specify this parameter, the command displays LDAP client configurations using the specified list of servers.

**[-ad-domain <TextNoCase>]** - Active Directory Domain

---

If you specify this parameter, the command displays LDAP client configurations using the specified domain to discover their list of LDAP servers.

**[-preferred-ad-servers <IP Address>, ...]** - Preferred Active Directory Servers

If you specify this parameter, the command displays LDAP client configurations using the specified list of preferred servers.

**[-bind-as-cifs-server {true|false}]** - Bind Using the Vserver's CIFS Credentials

If you specify this parameter, the command displays LDAP client configurations that bind using CIFS server credentials.

**[-schema <text>]** - Schema Template

If you specify this parameter, the command displays LDAP client configurations using the specified schema.

**[-port <integer>]** - LDAP Server Port

If you specify this parameter, the command displays LDAP client configurations using the specified server port.

**[-query-timeout <integer>]** - Query Timeout (sec)

If you specify this parameter, the command displays LDAP client configurations using the specified query timeout (in seconds).

**[-min-bind-level {anonymous|simple|sas}]** - Minimum Bind Authentication Level

If you specify this parameter, the command displays LDAP client configurations using the specified minimum bind level.

**[-bind-dn <ldap\_dn>]** - Bind DN (User)

If you specify this parameter, the command displays LDAP client configurations using the specified bind DN.

**[-base-dn <ldap\_dn>]** - Base DN

If you specify this parameter, the command displays LDAP client configurations using the specified base DN.

**[-base-scope {base|onelevel|subtree}]** - Base Search Scope

If you specify this parameter, the command displays LDAP client configurations using the specified base search scope.

**[-user-dn <ldap\_dn>]** - User DN (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified user DN.



---

**[-user-scope {base|onelevel|subtree}]** - User Search Scope (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using using the specified user search scope.

**[-group-dn <ldap\_dn>]** - Group DN (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified group DN.

**[-group-scope {base|onelevel|subtree}]** - Group Search Scope (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using using the specified group search scope.

**[-netgroup-dn <ldap\_dn>]** - Netgroup DN (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified netgroup DN.

**[-netgroup-scope {base|onelevel|subtree}]** - Netgroup Search Scope (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified netgroup search scope.

**[-is-owner {true|false}]** - Vserver Owns Configuration

If you set this parameter to true, the command displays LDAP client configurations with the Vservers which own them.

## Examples

The following example shows a summary of all of the LDAP client configurations available for Vserver vs1:

```
cluster1::> vserver services ldap show -vserver vs1
Vserver      Client      Configuration LDAP Servers      Active Directory Domain      Schema      Min Bind
Level
-----
vs1          corp        172.16.0.100    -                               RFC-2307    anonymous
vs1          corpnew     172.16.0.200    -                               RFC-2307    simple
```

---

## vserver services ldap client schema copy

Copy an existing LDAP schema template

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver services ldap client schema copy` command creates a new LDAP schema template from an existing one. In addition to an owned LDAP schema template, a Vserver administrator can also copy a cluster-wide LDAP schema template that is owned by the admin Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver for which you want to copy an existing LDAP schema template.

**-schema** <text> - Schema Template

This parameter specifies the name of the existing schema template you want to copy.

**-new-schema-name** <text> - New Schema Template Name

This parameter specifies the name of the schema template copy.

### Examples

The following example creates a copy of the RFC-2307 schema template and names it `corp-schema` for Vserver "vs1":

```
cluster1::> vserver services ldap client schema copy -vserver vs1 -schema  
RFC-2307 -new-schema-name corp-schema
```

## vserver services ldap client schema delete

Delete an LDAP schema template

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

---

The `vserver services ldap client schema delete` command deletes an LDAP schema template. A Vserver administrator can only delete templates owned by the Vserver.

Note:

You cannot delete the default schema templates.

## Parameters

**[-vserver <vserver name>]** - Vserver

This parameter specifies the name of Vserver owning the LDAP schema template you want to delete.

**-schema <text>** - Schema Template

This parameter specifies the name of the schema template you want to delete.

## Examples

The following example deletes a schema template named `corp-schema` owned by Vserver `vs1`:

```
cluster1::> vserver services ldap client schema delete -vserver vs1 -schema corp-schema
```

## vserver services ldap client schema modify

Modify an LDAP schema template

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver services ldap client schema modify` command modifies an existing LDAP schema template. You cannot modify the default schema templates. Create a copy of a default schema template using the `vserver services ldap client schema copy` command, and then modify the copy. A Vserver administrator can only modify templates owned by the Vserver.

## Parameters

**[-vserver <vserver name>]** - Vserver

---

This parameter specifies the name of the Vserver owning the LDAP schema template you want to modify.

**-schema <text>** - Schema Template

This parameter specifies the name of the schema template you want to modify.

**[-comment <text>]** - Comment

This parameter specifies a comment that describes the schema template.

**[-posix-account-object-class <text>]** - RFC 2307 posixAccount Object Class

This parameter specifies the RFC 2307 posixAccount object class name defined by the schema.

**[-posix-group-object-class <text>]** - RFC 2307 posixGroup Object Class

This parameter specifies the RFC 2307 posixGroup object class name defined by the schema.

**[-nis-netgroup-object-class <text>]** - RFC 2307 nisNetgroup Object Class

This parameter specifies the RFC 2307 nisNetgroup object class name defined by the schema.

**[-uid-attribute <text>]** - RFC 2307 uid Attribute

This parameter specifies the RFC 2307 uid attribute name defined by the schema.

**[-uid-number-attribute <text>]** - RFC 2307 uidNumber Attribute

This parameter specifies the RFC 2307 uidNumber attribute name defined by the schema.

**[-gid-number-attribute <text>]** - RFC 2307 gidNumber Attribute

This parameter specifies the RFC 2307 gidNumber attribute name defined by the schema.

**[-cn-group-attribute <text>]** - RFC 2307 cn (for Groups) Attribute

This parameter specifies the RFC 2307 cn (for Groups) attribute name defined by the schema.

**[-cn-netgroup-attribute <text>]** - RFC 2307 cn (for Netgroups) Attribute

This parameter specifies the RFC 2307 cn (for Netgroups) attribute name defined by the schema.

**[-user-password-attribute <text>]** - RFC 2307 userPassword Attribute

---

This parameter specifies the RFC 2307 userPassword attribute name defined by the schema.

**[-gecos-attribute <text>]** - RFC 2307 geCos Attribute

This parameter specifies the RFC 2307 geCos attribute name defined by the schema.

**[-home-directory-attribute <text>]** - RFC 2307 homeDirectory Attribute

This parameter specifies the RFC 2307 homeDirectory attribute name defined by the schema.

**[-login-shell-attribute <text>]** - RFC 2307 loginShell Attribute

This parameter specifies the RFC 2307 loginShell attribute name defined by the schema.

**[-member-uid-attribute <text>]** - RFC 2307 memberUid Attribute

This parameter specifies the RFC 2307 memberUid attribute name defined by the schema.

**[-member-nis-netgroup-attribute <text>]** - RFC 2307 memberNisNetgroup Attribute

This parameter specifies the RFC 2307 memberNisNetgroup attribute name defined by the schema.

**[-nis-netgroup-triple-attribute <text>]** - RFC 2307 nisNetgroupTriple Attribute

This parameter specifies the RFC 2307 nisNetgroupTriple attribute name defined by the schema.

**[-windows-account-attribute <text>]** - ONTAP Name Mapping windowsAccount Attribute

This parameter specifies the name mapping windowsAccount attribute name defined by the schema.

## Examples

The following example modifies the schema template called `corp-schema` owned by Vserver `vs1` to use `User` as the uid attribute name:

```
cluster1::> vsriver services ldap client schema modify -vsriver vs1 -schema corp-  
schema -uid-attribute User
```

## See Also

`vsriver services ldap client schema copy`

---

## vserver services ldap client schema show

Display LDAP schema templates

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ldap client schema show` command shows information about LDAP schema templates which a Vserver can access. An LDAP schema template created by a Vserver's administrator or by the cluster administrator for the Vserver is owned by the Vserver. A cluster-wide LDAP schema template is created by a cluster administrator by specifying the admin Vserver's name as a value to the `-vserver` parameter. In addition to its owned LDAP schema templates, a Vserver can access such cluster-wide LDAP schema templates.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays all LDAP schema templates that can be accessed by the specified Vserver.

**[-schema <text>]** - Schema Template

If you specify this parameter, the command displays the schema template with the specified name.

**[-comment <text>]** - Comment

If you specify this parameter, the command displays schema templates with the specified comment.

**[-posix-account-object-class <text>]** - RFC 2307 posixAccount Object Class

---

If you specify this parameter, the command displays schema templates with the specified posixAccount object class.

**[-posix-group-object-class <text>]** - RFC 2307 posixGroup Object Class

If you specify this parameter, the command displays schema templates with the specified posixGroup object class.

**[-nis-netgroup-object-class <text>]** - RFC 2307 nisNetgroup Object Class

If you specify this parameter, the command displays schema templates with the specified nisNetgroup object class.

**[-uid-attribute <text>]** - RFC 2307 uid Attribute

If you specify this parameter, the command displays schema templates with the specified uid attribute.

**[-uid-number-attribute <text>]** - RFC 2307 uidNumber Attribute

If you specify this parameter, the command displays schema templates with the specified uidNumber attribute.

**[-gid-number-attribute <text>]** - RFC 2307 gidNumber Attribute

If you specify this parameter, the command displays schema templates with the specified gidNumber attribute.

**[-cn-group-attribute <text>]** - RFC 2307 cn (for Groups) Attribute

If you specify this parameter, the command displays schema templates with the specified cn (for Groups) attribute.

**[-cn-netgroup-attribute <text>]** - RFC 2307 cn (for Netgroups) Attribute

If you specify this parameter, the command displays schema templates with the specified cn (for Netgroups) attribute.

**[-user-password-attribute <text>]** - RFC 2307 userPassword Attribute

If you specify this parameter, the command displays schema templates with the specified userPassword attribute.

**[-gecos-attribute <text>]** - RFC 2307 geCos Attribute

If you specify this parameter, the command displays schema templates with the specified geCos attribute.

**[-home-directory-attribute <text>]** - RFC 2307 homeDirectory Attribute

If you specify this parameter, the command displays schema templates with the specified homeDirectory attribute.

---

**[-login-shell-attribute <text>]** - RFC 2307 loginShell Attribute

If you specify this parameter, the command displays schema templates with the specified loginShell attribute.

**[-member-uid-attribute <text>]** - RFC 2307 memberUid Attribute

If you specify this parameter, the command displays schema templates with the specified memberUid attribute.

**[-member-nis-netgroup-attribute <text>]** - RFC 2307 memberNisNetgroup Attribute

If you specify this parameter, the command displays schema templates with the specified memberNisNetgroup attribute.

**[-nis-netgroup-triple-attribute <text>]** - RFC 2307 nisNetgroupTriple Attribute

If you specify this parameter, the command displays schema templates with the specified nisNetgroupTriple attribute.

**[-windows-account-attribute <text>]** - ONTAP Name Mapping windowsAccount Attribute

If you specify this parameter, the command displays schema templates with the specified windowsAccount attribute.

**[-is-owner {true|false}]** - Vserver Owns Schema

If you set this parameter to true, the command displays LDAP schema templates with the Vservers which own them.

## Examples

The following example shows a summary of all of the LDAP schema templates defined in the cluster that can be accessed by Vserver vs1:

```
cluster1::> vserver services ldap client schema show -vserver vs1
Vserver Schema Template Comment
-----
vs1      AD-SFU             Schema based on Active Directory Services for UNIX (read-
only)
vs1      RFC-2307           Schema based on RFC 2307 (read-only)
vs1      corp-schema       RFC 2307 schema based on the corporate schema
3 entries were displayed.
```



---

## vserver services ndmp generate-password

Generates NDMP password for a user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command is used to generate NDMP password for a given user in the specified Vserver context. The generated NDMP password is based on the user's login password. For this reason regenerate it whenever the user's login password changes. This command fails if a user does not exist for the Vserver.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Specify the Vserver context for which password is to be generated.

[-user <text>] - User

Specify the user name for which the NDMP password needs to be generated.

[-password <text>] - Password

The generated NDMP password string that is used for authentication.

### Examples

The following example shows the usage this command to generate NDMP password for a user belonging to a specific Vserver:

```
cluster1::> vserver services ndmp generate-password -vserver vservers1 -user user1
Vserver: vservers1
User: user1
Password: a9cCCUp32yjGmBiD
```

---

## vserver services ndmp kill-all

Kill all NDMP sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command terminates all NDMP sessions on a particular Vserver in the cluster.

### Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver name in which all NDMP sessions that are to be terminated are running.

### Examples

The following example shows how all NDMP sessions on the Vserver named vserver1 can be terminated:

```
cluster1::> vserver services ndmp kill-all -vserver vserver1
```

## vserver services ndmp kill

Kill the specified NDMP session

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command terminates a specific NDMP session on a particular Vserver in the cluster.

### Parameters

**-vserver** <vserver name> - Vserver

---

Specifies the Vserver in which the NDMP session that needs to be terminated is running.

<text> - Session Identifier

Session ID of the NDMP session. A session-id is a string used to identify a particular NDMP session.

## Examples

The following example shows how a specific NDMP session on the Vserver named vservers1 can be terminated:

```
cluster1::> vservers services ndmp kill 1000:8002 -vservers vservers1
```

## See Also

vservers services ndmp killsession

---

## vserver services ndmp modify

Modify NDMP Properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command is used to change NDMP options on Vservers.

One or more of the options specified in the parameters section can be modified for a specific Vserver, by this command. A short description of each of the options is provided in the parameters section.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

**[-maxversion** <integer>] - NDMP version

This option can be used to set the highest NDMP protocol version supported by the NDMP server . The only supported value is 4.

**[-ignore-ctime-enabled** {true|false}] - Ignore ctime

This option, when true, allows user to exclude files with ctime changed from storage system' incremental dumps since other processes like virus scanning often alter the ctime of files. When this option is false, backup on the Vserver will include all files with a change or modified time later then the last dump in the previous level dump. The default value is false. This option is persistent across reboots.

Most WIN32 APIs are often unaware of the "last changed time", ctime, they often incorrectly set a later time for files, causing these files to be included in the Vserver's incremental dumps, making the incremental dump very large. This is partially defying the purpose of having incremental dumps, since one uses incremental dumps to speed up the backup by only dumping files that were truly changed since the last backup.

The `-option-value` for this parameter should be true/false.

**[-offset-map-enable** {true|false}] - Enable offset map

This option is used to enable or disable generation of the inode offset map during NDMP based dump backups. The offset map is required to perform Enhanced Direct Access Restore (DAR) on the backup data. Enhanced DAR provides support for directory DAR

---

and DAR of files with NT streams. The default value for this option is true. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-tcpnodelay {true|false}]** - Enable tcp nodelay

Enables/Disables the TCPNODELAY configuration parameter for the socket between the Vserver and the DMA. When set to true, the Nagle algorithm is disabled and small packets are sent immediately rather than held and bundled with other small packets. This optimizes the system for response time rather than throughput.

This option becomes active when the next NDMP session starts. Existing sessions are unaffected. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-tcpwsize <integer>]** - TCP window size

This option can be used to change the TCP buffer size of the NDMP data connection. The minimum and maximum values are 8192(8K) and 262,144(256K), respectively. The default value for this option is 32768(32K).

This option is persistent across reboots.

The `-option-value` for this parameter should be a number between 8192(8K) and 262,144(256K).

**[-data-port-range <text>]** - Data port range

This option allows administrators to specify a port range on which the NDMP server can listen for data connections.

The format of this option is `start_port - end_port`. `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`. If a valid range is specified, NDMP uses a port within that range to listen for data connections. A listen request fails if no ports in the specified range are free.

This option is modifiable only from the admin Vserver context and the said option is applicable for all the data Vservers and the admin Vserver. For example, if the value of the above option is set with 2000-3000, the same value will be applicable throughout the cluster. The value `all` implies that any available port can be used to listen for data connections. The default value for this option is `all`. This option is persistent across reboots.

The `-option-value` for this option should be in the format `{<start_port>-<end port> | all }` - where `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`.

---

**[-backup-log-enable {true|false}]** - Enable backup log

Backup logging captures important events during dump/restore and records them in /mroot/etc/log/backup on the root volume. The option allows users to enable or disable this feature. The default value for this option is true. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-per-qtrees-exclude-enable {true|false}]** - Enable per qtrees exclusion

If this option is true, users can specify exclude list on a per qtrees basis to be excluded from backup. This exclude list will override any values already present due to 'EXCLUDE' environment variable. The user can specify the exclusion list through a `.exclude_list` file which resides at the root of the qtrees. The exclusion list can be a list of files or files that match a specified pattern. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-authtype <NDMP Authentication types>, ...]** - Authentication type

Allows the administrator to choose the authentication method. NDMP supports two authentication types: challenge and plaintext. The default of this option is challenge. This option is persistent across reboots.

The `-option-value` for this parameter can be {challenge | plaintext | challenge, plaintext | plaintext, challenge}.

**[-debug-enable {true|false}]** - Enable debug (privilege: advanced)

This option enables debug logging for NDMP. Debug messages will be logged to the ndmpd log file /mroot/etc/log/mlog/ndmpd.log. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-debug-filter <text>]** - Debug filter (privilege: advanced)

This option controls the NDMP modules for which debug logging is to be enabled. option-value can take five values for this option : all, none, normal, backend or "filter-expression".

all enables debug logging for all modules.

none disables debug logging for all modules. It is equivalent to modify `-vserver vservice_name -debug-enable false`.

normal is a shortcut option that enables debug logging for all modules except verbose and io\_loop. The equivalent filter string is `all-verbose-io_loop`.

backend is a short cut option that enables debug logging for all modules except verbose, io\_loop, ndmps and ndmpd. The equivalent filter string is all-verbose-io\_loop-ndmps-ndmpp.

(filter-expression) is a combination of one or more modules for which debug logs needs to be enabled. Multiple module names can be combined using following operators :

- - to remove the given module from the list of specified modules in the filter string. For example the filter all-ndmpp will enable debug logging for all modules but not ndmpp.
- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter ndmpp^mover^data will enable debug logging for ndmpp, mover and data.

The possible module names and a brief description is given below:-

Modules	Description
verbose	verbose message
io	I/O process loop
io_loop	I/O process loop verbose messages
ndmps	NDMP service
ndmpp	NDMP Protocol
rpc	General RPC service
fdc_rpc	RPC to FC driver service
auth	Authentication
mover	NDMP MOVER (tape I/O)
data	NDMP DATA (backup/restore)
scsi	NDMP SCSI (robot/tape ops)
bkup_rpc	RPC to Backup service client
bkup_rpc_s	RPC to Backup service server
cleaner	Backup/Mover session cleaner
conf	Debug configure/reconfigure
dblade	Dblade specific messages
timer	NDMP server timeout messages
vldb	VLDB service
smf	SMF Gateway messages
vol	VOL OPS service
sv	SnapVault NDMP extension
common	NDMP common state
ext	NDMP extensions messages
sm	SnapMirror NDMP extension
ndmprpc	NDMP Mhost RPC server

The default value for this option is none. This option is persistent across reboots.

The -option-value for this parameter can be {all | none | normal | backend |filter-expression}.

**[-dump-logical-find <text>]** - Enable logical find for dump (privilege: advanced)

This option specifies whether to follow inode-file walk or tree walk for phase I of the dump. Choosing inode-file walk or tree walk affects the performance of the dump. This option can take following values:

If default is specified, then level 0 and incremental volume as well as qtree dumps will use inode walk. All the subtree dumps will use tree walk.

---

If `always` is specified, all dumps will follow `treewalk`.

A comma-separated list of values in any combination from the following list:

- `vol_baseline`: Level 0 full volume backup will follow `treewalk`.
- `vol_incr`: Incremental full volume backup will follow `treewalk`.
- `qtree_baseline`: Level 0 qtree backup will follow `treewalk`.
- `qtree_incr`: Incremental qtree backup will follow `treewalk`.

The default value for this option is `default`. This option is persistent across reboots.

The `-option-value` for this parameter could be `{default | always | 'vol_baseline' | 'vol_baseline,qtree_baseline' | ...}`.

**`[-abort-on-disk-error {true|false}]`** - Enable abort on disk error (privilege: advanced)

If this option is `true`, dump will abort the backup operation on detection of irrecoverable data blocks in user files. If this option is `false`, dump will proceed with backup operation - even if irrecoverable data blocks in user files are detected. On detection of irrecoverable data blocks, dump will send a log message to DMA and also log an entry in `/mroot/etc/log/backup` file. The default value for this option is `false`. This option is persistent across reboots.

The `-option-value` for this parameter should be `true/false`.

**`[-fh-dir-retry-interval <integer>]`** - FH throttle value for dir (privilege: advanced)

NDMP protocol sends back file history information for all directories in phase 3 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle a slow reader, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The `-option-value` for this parameter should be a number.

**`[-fh-node-retry-interval <integer>]`** - FH throttle value for node (privilege: advanced)

NDMP protocol sends back file history information for all files in phase 4 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle slow reader conditions, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.



---

The `-option-value` for this parameter should be a number.

**`[-restore-vm-cache-size <integer>]`** - Restore VM file cache size (privilege: advanced)

This option mandates the number of WAFL buffers pinned in memory by various meta-files used by logical restore. The minimum and maximum values are 4 and 1024, respectively. The default value for this option is 64. This option is persistent across reboots.

Depending on the value of this option, various meta-files are assigned a number of WAFL buffers that need to be pinned in memory.

Meta-filename	Number of WAFL buffers to be pinned in memory
dumpmap	ndmpd.restore.vm_cache_size
filemap	ndmpd.restore.vm_cache_size
aclfile_map	ndmpd.restore.vm_cache_size
inomap	ndmpd.restore.vm_cache_size / 2
basemap	ndmpd.restore.vm_cache_size / 2
flipmap	ndmpd.restore.vm_cache_size / 2
revmap	ndmpd.restore.vm_cache_size / 2
clrimap	ndmpd.restore.vm_cache_size / 4
mfp_for_inotab	ndmpd.restore.vm_cache_size / 4
map	ndmpd.restore.vm_cache_size / 4
offsetfile_map	ndmpd.restore.vm_cache_size / 4

The `-option-value` for this parameter should be a number between 4 and 1024.

**`[-enable {true|false}]`** - Enable NDMP on vserver

When the option is set to true, the NDMP daemon handles requests, and when set to false, the NDMP daemon does not handle requests. Enabling and disabling the option is equivalent to executing the following commands: `vserver services ndmp on` and `vserver services ndmp off` respectively. This option is persistent across reboots. The default value of this option is false.

The `-option-value` for this parameter is either true or false.

**`[-preferred-interface-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}, ...]`** - Preferred interface role

This option allows the user to specify the preferred Logical Interface (LIF) role while establishing an NDMP data connection channel. The NDMP data server or the NDMP mover establishes a data channel from the node that owns the volume or the tape device respectively. This option is used on the node that owns the volume or the tape device. The order of IP addresses that are used to establish the data connection depends on the order of LIF roles specified in this option.

The default value for this option for the admin Vserver is `intercluster, cluster-mgmt, node-mgmt`

The default value for this option for a data Vserver is `intercluster, data`.

---

**[-secondary-debug-filter <text>]** - Secondary debug filter (privilege: advanced)

This option allows control on NDMP debug logging. This option takes a comma separated tag=value pairs. The supported tag is IPADDR which can be used to specify Vserver IP addresses for which NDMP debugging is required. If this option is set and the option `debug-enable` is set to true, then the debug-filter option is applicable to sessions whose control connection IP addresses match the IP addresses that are listed in the option. If this option is not set, the debug filter is applicable to all Vserver sessions. By default, this option does not have a value set.

## Examples

The following example show how to enable NDMP on a Vserver and set authorization type to plaintext :

```
cluster::> vserver services ndmp modify -vserver vs1 -enable true -authtype
plaintext
cluster::>
```

## vserver services ndmp off

Disable NDMP service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command is used to disable NDMP service on a specific Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

**[-maxversion** <integer>] - NDMP version

This option can be used to set the highest NDMP protocol version supported by the NDMP server . The only supported value is 4.

**[-ignore-ctime-enabled** {true|false}] - Ignore ctime

This option, when true, allows user to exclude files with ctime changed from storage system' incremental dumps since other processes like virus scanning often alter the ctime of files. When this option is false, backup on the Vserver will include all files with a

---

change or modified time later than the last dump in the previous level dump. The default value is false. This option is persistent across reboots.

Most WIN32 APIs are often unaware of the "last changed time", ctime, they often incorrectly set a later time for files, causing these files to be included in the Vserver's incremental dumps, making the incremental dump very large. This is partially defying the purpose of having incremental dumps, since one uses incremental dumps to speed up the backup by only dumping files that were truly changed since the last backup.

The `-option-value` for this parameter should be true/false.

**[-offset-map-enable {true|false}]** - Enable offset map

This option is used to enable or disable generation of the inode offset map during NDMP based dump backups. The offset map is required to perform Enhanced Direct Access Restore (DAR) on the backup data. Enhanced DAR provides support for directory DAR and DAR of files with NT streams. The default value for this option is true. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-tcpnodelay {true|false}]** - Enable tcp nodelay

Enables/Disables the TCPNODELAY configuration parameter for the socket between the Vserver and the DMA. When set to true, the Nagle algorithm is disabled and small packets are sent immediately rather than held and bundled with other small packets. This optimizes the system for response time rather than throughput.

This option becomes active when the next NDMP session starts. Existing sessions are unaffected. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-tcpwinsize <integer>]** - TCP window size

This option can be used to change the TCP buffer size of the NDMP data connection. The minimum and maximum values are 8192(8K) and 262,144(256K), respectively. The default value for this option is 32768(32K).

This option is persistent across reboots.

The `-option-value` for this parameter should be a number between 8192(8K) and 262,144(256K).

**[-data-port-range <text>]** - Data port range

This option allows administrators to specify a port range on which the NDMP server can listen for data connections.

---

The format of this option is `start_port - end_port start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`. If a valid range is specified, NDMP uses a port within that range to listen for data connections. A listen request fails if no ports in the specified range are free.

This option is modifiable only from the admin Vserver context and the said option is applicable for all the data Vservers and the admin Vserver. For example, if the value of the above option is set with 2000-3000, the same value will be applicable throughout the cluster. The value `all` implies that any available port can be used to listen for data connections. The default value for this option is `all`. This option is persistent across reboots.

The `-option-value` for this option should be in the format `{<start_port>-<end port> | all}` - where `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`.

**`[-backup-log-enable {true|false}]`** - Enable backup log

Backup logging captures important events during dump/restore and records them in `/mroot/etc/log/backup` on the root volume. The option allows users to enable or disable this feature. The default value for this option is `true`. This option is persistent across reboots.

The `-option-value` for this parameter should be `true/false`.

**`[-per-qtrees-exclude-enable {true|false}]`** - Enable per qtrees exclusion

If this option is `true`, users can specify exclude list on a per qtrees basis to be excluded from backup. This exclude list will override any values already present due to 'EXCLUDE' environment variable. The user can specify the exclusion list through a `.exclude_list` file which resides at the root of the qtrees. The exclusion list can be a list of files or files that match a specified pattern. The default value for this option is `false`. This option is persistent across reboots.

The `-option-value` for this parameter should be `true/false`.

**`[-authtype <NDMP Authentication types>, ...]`** - Authentication type

Allows the administrator to choose the authentication method. NDMP supports two authentication types: `challenge` and `plaintext`. The default of this option is `challenge`. This option is persistent across reboots.

The `-option-value` for this parameter can be `{challenge | plaintext | challenge, plaintext | plaintext, challenge}`.

**`[-debug-enable {true|false}]`** - Enable debug (privilege: advanced)

---

This option enables debug logging for NDMP. Debug messages will be logged to the ndmpd log file /mroot/etc/log/mlog/ndmpd.log . The default value for this option is false .This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-debug-filter <text>]** - Debug filter (privilege: advanced)

This option controls the NDMP modules for which debug logging is to be enabled. option-value can take five values for this option : all, none, normal, backend or "filter-expression".

all enables debug logging for all modules.

none disables debug logging for all modules. It is equivalent to modify `-vserver vsERVER_name -debug-enable false`.

normal is a shortcut option that enables debug logging for all modules except verbose and io\_loop. The equivalent filter string is `all-verbose-io_loop`.

backend is a short cut option that enables debug logging for all modules except verbose, io\_loop, ndmps and ndmpd. The equivalent filter string is `all-verbose-io_loop-ndmps-ndmpd`.

(filter-expression) is a combination of one or more modules for which debug logs needs to be enabled. Multiple module names can be combined using following operators :

- - to remove the given module from the list of specified modules in the filter string. For example the filter `all-ndmpps` will enable debug logging for all modules but not ndmpps.
- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter `ndmpps^mover^data` will enable debug logging for ndmpps, mover and data.

The possible module names and a brief description is given below:-

Modules	Description
verbose	verbose message
io	I/O process loop
io_loop	I/O process loop verbose messages
ndmps	NDMP service
ndmpps	NDMP Protocol
rpc	General RPC service
fdc_rpc	RPC to FC driver service
auth	Authentication
mover	NDMP MOVER (tape I/O)
data	NDMP DATA (backup/restore)
scsi	NDMP SCSI (robot/tape ops)
bkup_rpc	RPC to Backup service client
bkup_rpc_s	RPC to Backup service server
cleaner	Backup/Mover session cleaner
conf	Debug configure/reconfigure
dblade	Dblade specific messages
timer	NDMP server timeout messages
vldb	VLDB service

---

smf	SMF Gateway messages
vol	VOL OPS service
sv	SnapVault NDMP extension
common	NDMP common state
ext	NDMP extensions messages
sm	SnapMirror NDMP extension
ndmprpc	NDMP Mhost RPC server

---

The default value for this option is none. This option is persistent across reboots.

The `-option-value` for this parameter can be {all | none | normal | backend |'filter-expression'}.

**[-dump-logical-find <text>]** - Enable logical find for dump (privilege: advanced)

This option specifies whether to follow inode-file walk or tree walk for phase I of the dump. Choosing inode-file walk or tree walk affects the performance of the dump. This option can take following values:

If default is specified, then level 0 and incremental volume as well as qtree dumps will use inode walk. All the subtree dumps will use tree walk.

If always is specified, all dumps will follow treewalk.

A comma-separated list of values in any combination from the following list:

- vol\_baseline: Level 0 full volume backup will follow treewalk.
- vol\_incr: Incremental full volume backup will follow treewalk.
- qtree\_baseline: Level 0 qtree backup will follow treewalk.
- qtree\_incr: Incremental qtree backup will follow treewalk.

The default value for this option is default. This option is persistent across reboots.

The `-option-value` for this parameter could be {default | always | 'vol\_baseline' | 'vol\_baseline,qtree\_baseline' | ...}.

**[-abort-on-disk-error {true|false}]** - Enable abort on disk error (privilege: advanced)

If this option is true, dump will abort the backup operation on detection of irrecoverable data blocks in user files. If this option is false, dump will proceed with backup operation - even if irrecoverable data blocks in user files are detected. On detection of irrecoverable data blocks, dump will send a log message to DMA and also log an entry in /mroot/etc/log/backup file. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-fh-dir-retry-interval <integer>]** - FH throttle value for dir (privilege: advanced)

NDMP protocol sends back file history information for all directories in phase 3 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file

history being generated exceeds the amount being consumed by the DMA. To handle a slow reader, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The `-option-value` for this parameter should be a number.

**[-fh-node-retry-interval <integer>]** - FH throttle value for node (privilege: advanced)

NDMP protocol sends back file history information for all files in phase 4 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle slow reader conditions, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The `-option-value` for this parameter should be a number.

**[-restore-vm-cache-size <integer>]** - Restore VM file cache size (privilege: advanced)

This option mandates the number of WAFL buffers pinned in memory by various meta-files used by logical restore. The minimum and maximum values are 4 and 1024, respectively. The default value for this option is 64. This option is persistent across reboots.

Depending on the value of this option, various meta-files are assigned a number of WAFL buffers that need to be pinned in memory.

Meta-filename	Number of WAFL buffers to be pinned in memory
dumpmap	ndmpd.restore.vm_cache_size
filemap	ndmpd.restore.vm_cache_size
aclfile_map	ndmpd.restore.vm_cache_size
inomap	ndmpd.restore.vm_cache_size / 2
basemap	ndmpd.restore.vm_cache_size / 2
flipmap	ndmpd.restore.vm_cache_size / 2
revmap	ndmpd.restore.vm_cache_size / 2
clrimap	ndmpd.restore.vm_cache_size / 4
mfp_for_inotab	ndmpd.restore.vm_cache_size / 4
map	ndmpd.restore.vm_cache_size / 4
offsetfile_map	ndmpd.restore.vm_cache_size / 4

The `-option-value` for this parameter should be a number between 4 and 1024.

**[-enable {true|false}]** - Enable NDMP on vserver

When the option is set to true, the NDMP daemon handles requests, and when set to false, the NDMP daemon does not handle requests. Enabling and disabling the option is equivalent to executing the following commands: `vserver services ndmp on` and `vserver`

---

services ndmp off respectively. This option is persistent across reboots. The default value of this option is false.

The `-option-value` for this parameter is either true or false.

**[-preferred-interface-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}, ...]** - Preferred interface role

This option allows the user to specify the preferred Logical Interface (LIF) role while establishing an NDMP data connection channel. The NDMP data server or the NDMP mover establishes a data channel from the node that owns the volume or the tape device respectively. This option is used on the node that owns the volume or the tape device. The order of IP addresses that are used to establish the data connection depends on the order of LIF roles specified in this option.

The default value for this option for the admin Vserver is intercluster, cluster-mgmt, node-mgmt

The default value for this option for a data Vserver is intercluster, data.

**[-secondary-debug-filter <text>]** - Secondary debug filter (privilege: advanced)

This option allows control on NDMP debug logging. This option takes a comma separated tag=value pairs. The supported tag is IPADDR which can be used to specify Vserver IP addresses for which NDMP debugging is required. If this option is set and the option `debug-enable` is set to true, then the debug-filter option is applicable to sessions whose control connection IP addresses match the IP addresses that are listed in the option. If this option is not set, the debug filter is applicable to all Vserver sessions. By default, this option does not have a value set.

## Examples

The following example disables NDMP on a specific Vserver:

```
cluster::> vserver services ndmp off -vserver vs1
```

## See Also

vserver services ndmp modify



---

## vserver services ndmp on

Enable NDMP service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command is used to enable NDMP service on a specific Vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

**[-maxversion** <integer>] - NDMP version

This option can be used to set the highest NDMP protocol version supported by the NDMP server. The only supported value is 4.

**[-ignore-ctime-enabled** {true|false}] - Ignore ctime

This option, when true, allows user to exclude files with ctime changed from storage system' incremental dumps since other processes like virus scanning often alter the ctime of files. When this option is false, backup on the Vserver will include all files with a change or modified time later then the last dump in the previous level dump. The default value is false. This option is persistent across reboots.

Most WIN32 APIs are often unaware of the "last changed time", ctime, they often incorrectly set a later time for files, causing these files to be included in the Vserver's incremental dumps, making the incremental dump very large. This is partially defying the purpose of having incremental dumps, since one uses incremental dumps to speed up the backup by only dumping files that were truly changed since the last backup.

The `-option-value` for this parameter should be true/false.

**[-offset-map-enable** {true|false}] - Enable offset map

This option is used to enable or disable generation of the inode offset map during NDMP based dump backups. The offset map is required to perform Enhanced Direct Access Restore (DAR) on the backup data. Enhanced DAR provides support for directory DAR and DAR of files with NT streams. The default value for this option is true. This option is persistent across reboots.

---

The `-option-value` for this parameter should be true/false.

**`[-tcpnodelay {true|false}]`** - Enable tcp nodelay

Enables/Disables the TCPNODELAY configuration parameter for the socket between the Vserver and the DMA. When set to true, the Nagle algorithm is disabled and small packets are sent immediately rather than held and bundled with other small packets. This optimizes the system for response time rather than throughput.

This option becomes active when the next NDMP session starts. Existing sessions are unaffected. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**`[-tcpwinsize <integer>]`** - TCP window size

This option can be used to change the TCP buffer size of the NDMP data connection. The minimum and maximum values are 8192(8K) and 262,144(256K), respectively. The default value for this option is 32768(32K).

This option is persistent across reboots.

The `-option-value` for this parameter should be a number between 8192(8K) and 262,144(256K).

**`[-data-port-range <text>]`** - Data port range

This option allows administrators to specify a port range on which the NDMP server can listen for data connections.

The format of this option is `start_port - end_port`. `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`. If a valid range is specified, NDMP uses a port within that range to listen for data connections. A listen request fails if no ports in the specified range are free.

This option is modifiable only from the admin Vserver context and the said option is applicable for all the data Vservers and the admin Vserver. For example, if the value of the above option is set with 2000-3000, the same value will be applicable throughout the cluster. The value `all` implies that any available port can be used to listen for data connections. The default value for this option is `all`. This option is persistent across reboots.

The `-option-value` for this option should be in the format `{<start_port>-<end port> | all}` - where `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`.

**`[-backup-log-enable {true|false}]`** - Enable backup log

---

Backup logging captures important events during dump/restore and records them in /mroot/etc/log/backup on the root volume. The option allows users to enable or disable this feature. The default value for this option is true. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-per-qtrees-exclude-enable {true|false}]** - Enable per qtrees exclusion

If this option is true, users can specify exclude list on a per qtrees basis to be excluded from backup. This exclude list will override any values already present due to 'EXCLUDE' environment variable. The user can specify the exclusion list through a `.exclude_list` file which resides at the root of the qtrees. The exclusion list can be a list of files or files that match a specified pattern. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-authtype <NDMP Authentication types>, ...]** - Authentication type

Allows the administrator to choose the authentication method. NDMP supports two authentication types: challenge and plaintext. The default of this option is challenge. This option is persistent across reboots.

The `-option-value` for this parameter can be {challenge | plaintext | challenge, plaintext | plaintext, challenge}.

**[-debug-enable {true|false}]** - Enable debug (privilege: advanced)

This option enables debug logging for NDMP. Debug messages will be logged to the ndmpd log file /mroot/etc/log/mlog/ndmpd.log. The default value for this option is false. This option is persistent across reboots.

The `-option-value` for this parameter should be true/false.

**[-debug-filter <text>]** - Debug filter (privilege: advanced)

This option controls the NDMP modules for which debug logging is to be enabled. option-value can take five values for this option : all, none, normal, backend or "filter-expression".

all enables debug logging for all modules.

none disables debug logging for all modules. It is equivalent to modify `-vserver vservice_name -debug-enable false`.

normal is a shortcut option that enables debug logging for all modules except verbose and io\_loop. The equivalent filter string is `all-verbose-io_loop`.

backend is a short cut option that enables debug logging for all modules except verbose, io\_loop, ndmps and ndmpd. The equivalent filter string is all-verbose-io\_loop-ndmps-ndmpp.

(filter-expression) is a combination of one or more modules for which debug logs needs to be enabled. Multiple module names can be combined using following operators :

- - to remove the given module from the list of specified modules in the filter string. For example the filter all-ndmpp will enable debug logging for all modules but not ndmpp.
- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter ndmpp^mover^data will enable debug logging for ndmpp, mover and data.

The possible module names and a brief description is given below:-

Modules	Description
verbose	verbose message
io	I/O process loop
io_loop	I/O process loop verbose messages
ndmps	NDMP service
ndmpp	NDMP Protocol
rpc	General RPC service
fdc_rpc	RPC to FC driver service
auth	Authentication
mover	NDMP MOVER (tape I/O)
data	NDMP DATA (backup/restore)
scsi	NDMP SCSI (robot/tape ops)
bkup_rpc	RPC to Backup service client
bkup_rpc_s	RPC to Backup service server
cleaner	Backup/Mover session cleaner
conf	Debug configure/reconfigure
dblade	Dblade specific messages
timer	NDMP server timeout messages
vldb	VLDB service
smf	SMF Gateway messages
vol	VOL OPS service
sv	SnapVault NDMP extension
common	NDMP common state
ext	NDMP extensions messages
sm	SnapMirror NDMP extension
ndmprpc	NDMP Mhost RPC server

The default value for this option is none. This option is persistent across reboots.

The -option-value for this parameter can be {all | none | normal | backend |'filter-expression'}.

**[-dump-logical-find <text>]** - Enable logical find for dump (privilege: advanced)

This option specifies whether to follow inode-file walk or tree walk for phase I of the dump. Choosing inode-file walk or tree walk affects the performance of the dump. This option can take following values:

If default is specified, then level 0 and incremental volume as well as qtree dumps will use inode walk. All the subtree dumps will use tree walk.

---

If `always` is specified, all dumps will follow `treewalk`.

A comma-separated list of values in any combination from the following list:

- `vol_baseline`: Level 0 full volume backup will follow `treewalk`.
- `vol_incr`: Incremental full volume backup will follow `treewalk`.
- `qtree_baseline`: Level 0 qtree backup will follow `treewalk`.
- `qtree_incr`: Incremental qtree backup will follow `treewalk`.

The default value for this option is `default`. This option is persistent across reboots.

The `-option-value` for this parameter could be `{default | always | 'vol_baseline' | 'vol_baseline,qtree_baseline' | ...}`.

**`[-abort-on-disk-error {true|false}]`** - Enable abort on disk error (privilege: advanced)

If this option is `true`, dump will abort the backup operation on detection of irrecoverable data blocks in user files. If this option is `false`, dump will proceed with backup operation - even if irrecoverable data blocks in user files are detected. On detection of irrecoverable data blocks, dump will send a log message to DMA and also log an entry in `/mroot/etc/log/backup` file. The default value for this option is `false`. This option is persistent across reboots.

The `-option-value` for this parameter should be `true/false`.

**`[-fh-dir-retry-interval <integer>]`** - FH throttle value for dir (privilege: advanced)

NDMP protocol sends back file history information for all directories in phase 3 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle a slow reader, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The `-option-value` for this parameter should be a number.

**`[-fh-node-retry-interval <integer>]`** - FH throttle value for node (privilege: advanced)

NDMP protocol sends back file history information for all files in phase 4 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle slow reader conditions, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

---

The `-option-value` for this parameter should be a number.

**`[-restore-vm-cache-size <integer>]`** - Restore VM file cache size (privilege: advanced)

This option mandates the number of WAFL buffers pinned in memory by various meta-files used by logical restore. The minimum and maximum values are 4 and 1024, respectively. The default value for this option is 64. This option is persistent across reboots.

Depending on the value of this option, various meta-files are assigned a number of WAFL buffers that need to be pinned in memory.

Meta-filename	Number of WAFL buffers to be pinned in memory
dumpmap	ndmpd.restore.vm_cache_size
filemap	ndmpd.restore.vm_cache_size
aclfile_map	ndmpd.restore.vm_cache_size
inomap	ndmpd.restore.vm_cache_size / 2
basemap	ndmpd.restore.vm_cache_size / 2
flipmap	ndmpd.restore.vm_cache_size / 2
revmap	ndmpd.restore.vm_cache_size / 2
clrimap	ndmpd.restore.vm_cache_size / 4
mfp_for_inotab	ndmpd.restore.vm_cache_size / 4
map	ndmpd.restore.vm_cache_size / 4
offsetfile_map	ndmpd.restore.vm_cache_size / 4

The `-option-value` for this parameter should be a number between 4 and 1024.

**`[-enable {true|false}]`** - Enable NDMP on vserver

When the option is set to true, the NDMP daemon handles requests, and when set to false, the NDMP daemon does not handle requests. Enabling and disabling the option is equivalent to executing the following commands: `vserver services ndmp on` and `vserver services ndmp off` respectively. This option is persistent across reboots. The default value of this option is false.

The `-option-value` for this parameter is either true or false.

**`[-preferred-interface-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}, ...]`** - Preferred interface role

This option allows the user to specify the preferred Logical Interface (LIF) role while establishing an NDMP data connection channel. The NDMP data server or the NDMP mover establishes a data channel from the node that owns the volume or the tape device respectively. This option is used on the node that owns the volume or the tape device. The order of IP addresses that are used to establish the data connection depends on the order of LIF roles specified in this option.

The default value for this option for the admin Vserver is `intercluster, cluster-mgmt, node-mgmt`

The default value for this option for a data Vserver is `intercluster, data`.

---

**[-secondary-debug-filter <text>]** - Secondary debug filter (privilege: advanced)

This option allows control on NDMP debug logging. This option takes a comma separated tag=value pairs. The supported tag is IPADDR which can be used to specify Vserver IP addresses for which NDMP debugging is required. If this option is set and the option `debug-enable` is set to true, then the debug-filter option is applicable to sessions whose control connection IP addresses match the IP addresses that are listed in the option. If this option is not set, the debug filter is applicable to all Vserver sessions. By default, this option does not have a value set.

## Examples

The following example enables NDMP service on a specific Vserver:

```
cluster::> vserver services ndmp on -vserver vs1
```

## See Also

`vserver services ndmp modify`

---

## vserver services ndmp probe

Display list of NDMP sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `system services ndmp probe` command displays diagnostic information about NDMP sessions belonging to a specific Vserver in the cluster. The following fields are displayed for each of the sessions:

- Vserver
- Session identifier
- NDMP version
- Session authorized
- Data state
- Data operation
- Data server halt reason
- Data server connect type
- Data server connect address
- Data server connect port
- Data bytes processed
- Mover state
- Mover mode
- Mover pause reason
- Mover halt reason
- Mover record size
- Mover record number
- Mover bytes moved
- Mover seek position



- 
- Mover bytes left to read
  - Mover window offset
  - Mover window length
  - Mover position
  - Mover SetRecordSize flag
  - Mover SetWindow flag
  - Mover connect type
  - Mover connect address
  - Mover connect port
  - Effective host
  - NDMP client address
  - NDMP client port
  - SCSI device ID
  - SCSI hostadapter
  - SCSI target ID
  - SCSI LUN ID
  - Tape device
  - Tape mode
  - Node

## Parameters

**-vserver** <vserver name> - Vserver

Specifies the Vserver context in which NDMP sessions are running.

**-session-id** <text> - Session Identifier

If this parameter is specified, the command displays information about a specific NDMP session. A session-id is a string used to identify a particular NDMP session.

## Examples

The following example displays diagnostic information about all the sessions in the cluster:

---

```
cluster1::> vserver services ndmp probe
```

```
    Vserver Name: vserver1
    Session Identifier: 1000:7445
      NDMP Version: 4
    Session Authorized: true
      Data State: IDLE
    Data Operation: NOACTION
Data Server Halt Reason: NA
....
...

    Vserver Name: vserver2
    Session Identifier: 1000:7446
      NDMP Version: 4
    Session Authorized: true
      Data State: IDLE
    Data Operation: NOACTION
Data Server Halt Reason: NA
....
...
```

The following example displays diagnostic information of sessions associated with Vserver vserver1 only:

```
cluster1::> vserver services ndmp probe -vserver vserver1
```

```
    Vserver Name: vserver1
    Session Identifier: 1000:7445
      NDMP Version: 4
    Session Authorized: true
      Data State: IDLE
    Data Operation: NOACTION
Data Server Halt Reason: NA
....
...
....
...
....
...
```

## See Also

vserver services ndmp status    system services ndmp probe

---

## vserver services ndmp show

Display NDMP Properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command is used to display NDMP options on Vservers.

A combination of parameters can be optionally specified so as to list only a subset of Vservers where specific values of NDMP options are met. A short description of each of the options is provided in the parameters section.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays NDMP options for that Vserver alone.

[-maxversion <integer>] - NDMP version

If this parameter is specified, the command displays NDMP options for Vservers where the highest NDMP protocol version supported matches the specified input value. The only supported value is 4.

[-ignore-ctime-enabled {true|false}] - Ignore ctime

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `ignore-ctime-enabled` matches the specified input value.

This option, when true, allows user to exclude files with ctime changed from storage system' incremental dumps since other processes like virus scanning often alter the ctime of files. When this option is false, backup on the Vserver will include all files with a

---

change or modified time later than the last dump in the previous level dump. The default value is false. This option is persistent across reboots.

Most WIN32 APIs are often unaware of the "last changed time", ctime, they often incorrectly set a later time for files, causing these files to be included in the Vserver's incremental dumps, making the incremental dump very large. This is partially defying the purpose of having incremental dumps, since one uses incremental dumps to speed up the backup by only dumping files that were truly changed since the last backup.

The possible value for this parameter is either true or false.

**[-offset-map-enable {true|false}]** - Enable offset map

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `offset-map-enable` matches the specified input value.

This option is used to enable or disable generation of the inode offset map during NDMP based dump backups. The offset map is required to perform Enhanced Direct Access Restore (DAR) on the backup data. Enhanced DAR provides support for directory DAR and DAR of files with NT streams. The default value for this option is true. This option is persistent across reboots.

The possible value for this parameter is either true or false.

**[-tcpnodelay {true|false}]** - Enable tcp nodelay

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `tcpnodelay` matches the specified input value.

This parameter Enables/Disables the TCPNODELAY configuration parameter for the socket between the Vserver and the DMA. When set to true, the Nagle algorithm is disabled and small packets are sent immediately rather than held and bundled with other small packets. This optimizes the system for response time rather than throughput.

This option becomes active when the next NDMP session starts. Existing sessions are unaffected. The default value for this option is false. This option is persistent across reboots.

The possible value for this parameter is either true or false.

**[-tcpwinsize <integer>]** - TCP window size

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `tcpwinsize` matches the specified input value.

This option shows the TCP buffer size of the NDMP data connection. The minimum and maximum values are 8192(8K) and 262,144(256K), respectively. The default value for this option is 32768(32K).

---

This option is persistent across reboots.

The possible value for this parameter is a number between 8192(8K) and 262,144(256K).

**[-data-port-range <text>] - Data port range**

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `data-port-range` matches the specified input value.

This option shows the port range on which the NDMP server can listen for data connections.

The format of this option is `start_port - end_port` `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`. If a valid range is specified, NDMP uses a port within that range to listen for data connections. A listen request fails if no ports in the specified range are free.

This option is modifiable only from the admin Vserver context and the said option is applicable for all the data Vservers and the admin Vserver. For example, if the value of the above option is set with 2000-3000, the same value will be applicable throughout the cluster. The value `all` implies that any available port can be used to listen for data connections. The default value for this option is `all`. This option is persistent across reboots.

The value for this option is displayed in the format `{<start_port>-<end port> | all }` where `start_port`, `end_port` can have values between [1024-65535]; `start_port` must be lesser than or equal to `end_port`.

**[-backup-log-enable {true|false}] - Enable backup log**

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `>backup-log-enable` matches the specified input value.

Backup logging captures important events during dump/restore and records them in `/mroot/etc/log/backup` on the root volume. The default value for this option is `true`. This option is persistent across reboots.

The possible value for this parameter is `true/false`.

**[-per-qtree-exclude-enable {true|false}] - Enable per qtree exclusion**

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `per-qtree-exclude-enable` matches the specified input value.

If this option is `true`, users can specify exclude list on a per qtree basis to be excluded from backup. This exclude list will override any values already present due to 'EXCLUDE' environment variable . The user can specify the exclusion list through a `.exclude_list` file which resides at the root of the qtree. The exclusion list can be a list

---

of files or files that match a specified pattern. The default value for this option is false. This option is persistent across reboots.

The possible value for this parameter is either true or false.

**[-authtype <NDMP Authentication types>, ...]** - Authentication type

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `authtype` matches the specified input value.

Allows the administrator to choose the authentication method. NDMP supports two authentication types: challenge and plaintext. The default of this option is challenge. This option is persistent across reboots.

The possible value for this parameter can be {challenge | plaintext | challenge, plaintext | plaintext, challenge}.

**[-debug-enable {true|false}]** - Enable debug (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `debug-enable` matches the specified input value.

This option enables debug logging for NDMP. Debug messages will be logged to the `ndmpd` log file `/mroot/etc/log/mlog/ndmpd.log`. The default value for this option is false. This option is persistent across reboots.

The possible value for this parameter is either true or false.

**[-debug-filter <text>]** - Debug filter (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `debug-filter` matches the specified input value.

This option controls the NDMP modules for which debug logging is to be enabled. option-value can take five values for this option : all, none, normal, backend or "filter-expression".

all enables debug logging for all modules.

none disables debug logging for all modules. It is equivalent to modify `-vserver vserver_name -debug-enable false`.

normal is a shortcut option that enables debug logging for all modules except verbose and `io_loop`. The equivalent filter string is `all-verbose-io_loop`.

backend is a short cut option that enables debug logging for all modules except verbose, `io_loop`, `ndmps` and `ndmpd`. The equivalent filter string is `all-verbose-io_loop-ndmps-ndmpp`.

(filter-expression) is a combination of one or more modules for which debug logs needs to be enabled. Multiple module names can be combined using following operators :

- - to remove the given module from the list of specified modules in the filter string. For example the filter all-ndmpp will enable debug logging for all modules but not ndmpp.
- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter ndmpp^mover^data will enable debug logging for ndmpp, mover and data.

The possible module names and a brief description is given below:-

Modules	Description
verbose	verbose message
io	I/O process loop
io_loop	I/O process loop verbose messages
ndmps	NDMP service
ndmpp	NDMP Protocol
rpc	General RPC service
fdc_rpc	RPC to FC driver service
auth	Authentication
mover	NDMP MOVER (tape I/O)
data	NDMP DATA (backup/restore)
scsi	NDMP SCSI (robot/tape ops)
bkup_rpc	RPC to Backup service client
bkup_rpc_s	RPC to Backup service server
cleaner	Backup/Mover session cleaner
conf	Debug configure/reconfigure
dblade	Dblade specific messages
timer	NDMP server timeout messages
vldb	VLDB service
smf	SMF Gateway messages
vol	VOL OPS service
sv	SnapVault NDMP extension
common	NDMP common state
ext	NDMP extensions messages
sm	SnapMirror NDMP extension
ndmprpc	NDMP Mhost RPC server

The default value for this option is none. This option is persistent across reboots.

The possible value for this parameter can be {all | none | normal | backend |'filter-expression'}.

**[-dump-logical-find <text>]** - Enable logical find for dump (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for dump-logical-find matches the specified input value.

This option specifies whether to follow inode-file walk or tree walk for phase I of the dump. Choosing inode-file walk or tree walk affects the performance of the dump. This option can take following values:

If default is specified, then level 0 and incremental volume as well as qtree dumps will use inode walk. All the subtree dumps will use tree walk.

If always is specified, all dumps will follow treewalk.

A comma-separated list of values in any combination from the following list:

- 
- `vol_baseline`: Level 0 full volume backup will follow treewalk.
  - `vol_incr`: Incremental full volume backup will follow treewalk.
  - `qtree_baseline`: Level 0 qtree backup will follow treewalk.
  - `qtree_incr`: Incremental qtree backup will follow treewalk.

The default value for this option is default. This option is persistent across reboots.

The possible value for this parameter could be {default | always | 'vol\_baseline' | 'vol\_baseline,qtree\_baseline' | ...}.

**`[-abort-on-disk-error {true|false}]`** - Enable abort on disk error (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `abort-on-disk-error` matches the specified input value.

If this option is true, dump will abort the backup operation on detection of irrecoverable data blocks in user files. If this option is false, dump will proceed with backup operation - even if irrecoverable data blocks in user files are detected. On detection of irrecoverable data blocks, dump will send a log message to DMA and also log an entry in `/mroot/etc/log/backup` file. The default value for this option is false. This option is persistent across reboots.

The value for this parameter is either true or false.

**`[-fh-dir-retry-interval <integer>]`** - FH throttle value for dir (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `fh-dir-retry-interval` matches the specified input value.

NDMP protocol sends back file history information for all directories in phase 3 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle a slow reader, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The value for this parameter is a number.

**`[-fh-node-retry-interval <integer>]`** - FH throttle value for node (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `fh-node-retry-interval` matches the specified input value.

NDMP protocol sends back file history information for all files in phase 4 of dump to DMA. In the presence of slow DMA or high latency networks, the amount of file history being generated exceeds the amount being consumed by the DMA. To handle



---

slow reader conditions, a flow control mechanism is now introduced where file history generation is throttled when a DMA is slow in consuming them. The value for this option indicates how frequently should the file history be resent if it was throttled. The default value is 250 milliseconds. This option is persistent across reboots.

The value for this parameter is a number.

**[-restore-vm-cache-size <integer>]** - Restore VM file cache size (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `restore-vm-cache-size` matches the specified input value.

This option mandates the number of WAFL buffers pinned in memory by various meta-files used by logical restore. The minimum and maximum values are 4 and 1024, respectively. The default value for this option is 64. This option is persistent across reboots.

Depending on the value of this option, various meta-files are assigned a number of WAFL buffers that need to be pinned in memory.

Meta-filename	Number of WAFL buffers to be pinned in memory
dumpmap	ndmpd.restore.vm_cache_size
filemap	ndmpd.restore.vm_cache_size
aclfile_map	ndmpd.restore.vm_cache_size
inomap	ndmpd.restore.vm_cache_size / 2
basemap	ndmpd.restore.vm_cache_size / 2
flipmap	ndmpd.restore.vm_cache_size / 2
revmap	ndmpd.restore.vm_cache_size / 2
clrimap	ndmpd.restore.vm_cache_size / 4
mfp_for_inotab	ndmpd.restore.vm_cache_size / 4
map	ndmpd.restore.vm_cache_size / 4
offsetfile_map	ndmpd.restore.vm_cache_size / 4

The possible value for this parameter is a number between 4 and 1024.

**[-enable {true|false}]** - Enable NDMP on vserver

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `enable` matches the specified input value.

When the option is set to true, the NDMP daemon handles requests, and when set to false, the NDMP daemon does not handle requests. Enabling and disabling the option is equivalent to executing the following commands: `vserver services ndmp on` and `vserver services ndmp off` respectively. This option is persistent across reboots. The default value of this option is false.

The value for this parameter is either true or false.

**[-preferred-interface-role {cluster|data|node-mgmt|intercluster|cluster-mgmt}, ...]** - Preferred interface role

---

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `preferred-interface-role` matches the specified input value.

This option allows the user to specify the preferred Logical Interface (LIF) role while establishing an NDMP data connection channel. The NDMP data server or the NDMP mover establishes a data channel from the node that owns the volume or the tape device respectively. This option is used on the node that owns the volume or the tape device. The order of IP addresses that are used to establish the data connection depends on the order of LIF roles specified in this option.

The default value for this option for the admin Vserver is `intercluster`, `cluster-mgmt`, `node-mgmt`

The default value for this option for a data Vserver is `intercluster`, `data`.

**[-secondary-debug-filter <text>]** - Secondary debug filter (privilege: advanced)

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `secondary-debug-filter` matches the specified input value.

This option allows control on NDMP debug logging. This option takes a comma separated tag=value pairs. The supported tag is `IPADDR` which can be used to specify Vserver IP addresses for which NDMP debugging is required. If this option is set and the option `debug-enable` is set to `true`, then the `debug-filter` option is applicable to sessions whose control connection IP addresses match the IP addresses that are listed in the option. If this option is not set, the debug filter is applicable to all Vserver sessions. By default, this option does not have a value set.

## Examples

The following example displays NDMP options for the Vserver(s).

```
cluster::> vserver services ndmp show
VServer      Enabled  Authentication type
-----
cluster      true    plaintext
vs1          true    plaintext
vs2          true    plaintext
3 entries were displayed.
cluster::>
```

The following example displays detailed NDMP options for a Vserver.

```
cluster::*> vserver services ndmp show -vserver vs1 -instance
Vserver: vs1
NDMP version: 4
Ignore ctime: false
Enable offset map: true
Enable tcp nodelay: false
TCP window size: 32768
Data port range: all
Enable backup log: true
Enable per qtree exclusion: false
Authentication type: plaintext
Enable debug: false
Debug filter: none
Enable logical find for dump: default
```

---

```
    Enable abort on disk error: false
    FH throttle value for dir: 250
    FH throttle value for node: 500
    Restore VM file cache size: 64
Enable logging of VM stats for dump: false
    Enable NDMP on vserver: true
    Preferred interface role: intercluster, data
    Secondary debug filter: -

cluster::*>
```

---

## vserver services ndmp status

Display list of NDMP sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services ndmp status` command lists NDMP sessions belonging to a specific Vserver in the cluster. By default it lists the following details about the active sessions:

- Vserver Name
- Session ID

A combination of parameters can be optionally supplied so as to list only those sessions which match specific conditions. A short description of each of the parameter is provided in the parameters section.

### Parameters

{ [-**fields** <fieldname>, ...]

This optional parameter specifies which all additional fields to display. Any combination of the following fields are valid:

- ndmp-version
- session-authorized
- data-state
- data-operation
- data-halt-reason
- data-con-addr-type
- data-con-addr
- data-con-port
- data-bytes-processed
- mover-state

- 
- mover-mode
  - mover-pause-reason
  - mover-halt-reason
  - mover-record-size
  - mover-record-num
  - mover-bytes-moved
  - mover-seek-position
  - mover-bytes-left-to-read
  - mover-window-offset
  - mover-window-length
  - mover-position
  - mover-setrecordsize-flag
  - mover-setwindow-flag
  - mover-con-addr-type
  - mover-con-addr
  - mover-con-port
  - eff-host
  - client-addr
  - client-port
  - spt-device-id
  - spt-ha
  - spt-scsi-id
  - spt-scsi-lun
  - tape-device
  - tape-modes
  - node

| [-instance ] }

---

If this parameter is specified, the command displays detailed information about all the active sessions.

**[-vserver <vserver name>]** - Vserver

Specifies the Vserver context in which NDMP sessions are running.

**[-session-id <text>]** - Session Identifier

If this parameter is specified, the command displays information about specific NDMP session. A session-id is a string used to identify a particular NDMP session.

**[-ndmp-version <integer>]** - NDMP Version

This parameter refers to the NDMP protocol version being used in the session.

**[-session-authorized {true|false}]** - Session Authorized

This field indicates whether an NDMP session is authenticated or not.

**[-data-state <component state>]** - Data State

This field identifies the current state of the data server's state machine.

**[-data-operation <data operation>]** - Data Operation

This field identifies the data server's current operation.

**[-data-halt-reason <halt reason>]** - Data Server Halt Reason

This field identifies the event that caused the data server state machine to enter the HALTED state.

**[-data-con-addr-type <address type>]** - Data Server Connect Type

This field specifies the type of data connection established by the data server. The data connection can be established locally within a given system or between remote networked systems.

**[-data-con-addr <text>]** - Data Server Connect Address

This specifies the connection endpoint information for the data server's data connection.

**[-data-con-port <integer>]** - Data Server Connect Port

This specifies the TCP/IP port that the data server will use when establishing a data connection.

**[-data-bytes-processed <integer>]** - Data Bytes Processed

This field represents the cumulative number of data stream bytes transferred between the backup or recovery method and the data connection during the current data operation.

---

**[-mover-state <component state>]** - Mover State

This parameter identifies the current state of the NDMP tape server's mover state machine.

**[-mover-mode <mover mode>]** - Mover Mode

This parameter identifies the direction of the mover data transfer.

**[-mover-pause-reason <pause reason>]** - Mover Pause Reason

This parameter identifies the event that caused the mover state machine to enter the PAUSED state.

**[-mover-halt-reason <halt reason>]** - Mover Halt Reason

This integer field identifies the event that caused the mover state machine to enter the HALTED state.

**[-mover-record-size <integer>]** - Mover Record Size

This field represents the current mover record size in bytes.

**[-mover-record-num <integer>]** - Mover Record Number

This field represents the last tape record processed by the mover.

**[-mover-bytes-moved <integer>]** - Mover Bytes Moved

This field represents the cumulative number of data stream bytes written to the data connection or the number of data stream bytes read from the data connection and written to the tape subsystem, depending on the mode of mover operation.

**[-mover-seek-position <integer>]** - Mover Seek Position

This field represents the data stream offset of the first byte the DMA requested the mover to transfer to the data connection during a mover read operation.

**[-mover-bytes-left-to-read <integer>]** - Mover Bytes Left to Read

This field represents the number of data bytes remaining to be transferred to the data connection to satisfy the current NDMP\_MOVER\_READ request.

**[-mover-window-offset <integer>]** - Mover Window Offset

This field represents the absolute offset of the first byte of the mover window within the overall data stream.

**[-mover-window-length <integer>]** - Mover Window Length

This field represents the length of the current mover window in bytes.

**[-mover-position <integer>]** - Mover Position

---

This parameter can be used to list only those sessions, whose mover position matches a specific value. Mover-position should be an integer.

**[-mover-setrecordsize-flag {true|false}]** - Mover SetRecordSize Flag

This field is used by the DMA to establish the record size used for mover-initiated tape read and write operations.

**[-mover-setwindow-flag {true|false}]** - Mover SetWindow Flag

This flag represents whether a mover window has been set or not. A mover window represents the portion of the overall backup stream that is accessible to the mover without intervening DMA tape manipulation.

**[-mover-con-addr-type <address type>]** - Mover Connect Type

This field specifies the type of data connection established by the mover. The data connection can be established locally within a given system or between remote networked systems.

**[-mover-con-addr <text>]** - Mover Connect Address

This specifies the endpoint address or addresses that the mover will use when establishing a data connection.

**[-mover-con-port <integer>]** - Mover Connect Port

This specifies the TCP/IP port that the mover will use when establishing a data connection.

**[-eff-host <host type>]** - Effective Host

This field indicates the host context in which the NDMP session runs. The valid values are: PRIMARY or PARTNER.

**[-client-addr <text>]** - NDMP Client Address

This parameter specifies the client's IP address.

**[-client-port <integer>]** - NDMP Client Port

This parameter specifies the client's port number.

**[-spt-device-id <text>]** - SCSI Device ID

This parameter specifies the SCSI device ID.

**[-spt-ha <integer>]** - SCSI Host Adapter

This parameter specifies the SCSI host adapter.

**[-spt-scsi-id <integer>]** - SCSI Target ID



---

This parameter specifies the SCSI target.

**[-spt-scsi-lun <integer>]** - SCSI LUN ID

This parameter specifies the SCSI LUN ID.

**[-tape-device <text>]** - Tape Device

This parameter specifies the name to identify the tape device.

**[-tape-mode <mover mode>]** - Tape Mode

This parameter specifies the mode in which tapes are opened.

**[-node {<nodename>|local}]** - Node

If this parameter is specified, the command displays information about the sessions running on the specified node only. Node should be a valid node name.

## Examples

The following example displays all the NDMP sessions on the cluster:

```
cluster1::> vservice services ndmp status
              Session
      Vserver   Id
-----
      vservice1 1000:7445
      vservice2 1000:7446
      vservice2 1000:7447
3 entries were displayed.
```

The following example shows how to display only the sessions running belonging to Vserver vservice2:

```
cluster1::> vservice services ndmp status -vservice vservice2
              Session
      Vserver   Id
-----
      vservice2 1000:7446
      vservice2 1000:7447
2 entries were displayed.
```

---

## vserver services ndmp log start

Start logging for the specified NDMP session

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command is used to start logging on an active NDMP session on a vservers.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

**-session-id** <text> - Session Identifier

This parameter specifies the NDMP session-id on which logging needs to be started.

**-filter** <text> - Level Filter

Use this parameter to specify the filter for a particular session ID. This parameter controls the NDMP modules for which logging is to be enabled. This parameter can take five values. They are as follow : all, none, normal, backend or "filter-expression". The default value for this is none.

- all turns on logging for all modules.
- none disables logging for all modules.
- normal is a short cut parameter that enables logging for all modules except verbose and io\_loop. The equivalent filter string is all-verbose-io\_loop
- backend is a short cut parameter that enables logging for all modules except verbose, io\_loop, ndmps and ndmpd. The equivalent filter string is all-verbose-io\_loop-ndmps-ndmpd
- (filter-expression) is a combination of one or more modules for which logs needs to be enabled. Multiple module names can be combined using following operators :
  - - to remove the given module from the list of specified modules in the filter string. For example the filter all-ndmpp will enable logging for all modules but not ndmpp.

- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter ndmpp^mover^data will enable logging for ndmpp, mover and data.

The possible module names and a brief description is given below:

+-----+   +-----+		Modules	Description
messages		verbose	verbose message
		io	I/O process loop
		io_loop	I/O process loop verbose
		ndmps	NDMP service
		ndmpp	NDMP Protocol
		rpc	General RPC service
		fdc_rpc	RPC to FC driver service
restore) ops) client server cleaner reconfigure		auth	Authentication
		mover	NDMP MOVER (tape I/O)
		data	NDMP DATA (backup/
		scsi	NDMP SCSI (robot/tape
		bkup_rpc	RPC to Backup service
		bkup_rpc_s	RPC to Backup service
		cleaner	Backup/Mover session
messages		conf	Debug configure/
		dblade	Dblade specific messages
		timer	NDMP server timeout
		vldb	VLDB service
		smf	SMF Gateway messages
		vol	VOL OPS service
		sv	SnapVault NDMP extension
extension		common	NDMP common state
		ext	NDMP extensions messages
		sm	SnapMirror NDMP
		ndmprpc	NDMP Mhost RPC server

## Examples

The following example shows how to start logging on a specific NDMP session 1000:35512, running on vserver cluster1-01 with filter all.

---

```
cluster1-01 -session-id 1000:35512 -filter all cluster1::*> vserver services ndmp log start -vserver
```

## vserver services ndmp log stop

Stop logging for the specified NDMP session

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

This command is used to stop logging on an active NDMP session on a vserver.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the name of the Vserver.

**-session-id** <text> - Session Identifier

This parameter specifies the NDMP session-id on which logging needs to be stopped.

### Examples

The following example shows how to stop logging on a specific NDMP session 1000:35512 , running on vserver cluster1-01.

```
cluster1-01 -session-id 1000:35512 cluster1::*> vserver services ndmp log stop -vserver
```

## vserver services netgroup load

Load netgroup definitions from a URI

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services netgroup load` command loads netgroup definitions from a uniform resource identifier (URI) to a specified Vserver. You can load from a netgroup file at a FTP or a HTTP location (source URI) using the respective protocol.

---

## Parameters

**-vserver** <vserver> - Vserver

This parameter specifies the Vserver for which you want to load netgroup definitions.

**-source** {(ftp|http):||(hostname|IPv4 Address|'IPv6 Address')}...} - URI to load from

This parameter specifies the source URI from which you want to load netgroup definitions. You can load from a URI either using the FTP or the HTTP protocol.

## Examples

The following example loads netgroup definitions into a Vserver named vs1 from the file netgroup1 at FTP location ftp://ftp.example.com.

```
cluster1::> vsserver services netgroup load -vserver vs1 -source ftp://  
ftp.example.com/netgroup1
```

## vserver services netgroup status

Display local netgroup definitions status

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver services netgroup status` command displays the status of local netgroup definitions across a cluster. This enables you to verify that netgroup definitions are consistent across all nodes that back a Vserver into which netgroup definitions have been loaded.

The command displays the following information:

- Vserver name
- Node name
- Load time for netgroup definitions
- Hash value of the netgroup definitions

## Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

If you specify this parameter, the command displays netgroup status only for the specified Vserver.

**[-node {<nodename>|local}]** - Node

If you specify this parameter, the command displays netgroup status only for the specified node.

**[-timestamp <MM/DD/YYYY HH:MM:SS>]** - Load Time

If you specify this parameter, the command displays status only for the netgroup definitions that were loaded at the specified time. Specify time in the format MM/DD/YYYY HH:MM:SS. Note that the load time stamps for identical definitions are different on different nodes, because each node downloads the definitions from the URI individually.

**[-hashvalue <text>]** - Hash Value

If you specify this parameter, the command displays status only for the netgroup definitions that have the specified hash value. Note that the primary purpose of the command is to verify that the definitions on all nodes have the same hash value, so querying on a specific hash value is not useful in most cases.

## Examples

The following example displays netgroup definition status for all Vservers:

```
cluster1::*> vserver services netgroup status
Vserver   Node      Load Time      Hash Value
-----
vs1
    node1    9/20/2008 16:04:55 e6cb38ec1396a280c0d2b77e3a84eda2
    node2    9/20/2008 16:04:53 e6cb38ec1396a280c0d2b77e3a84eda2
vs2
    node3    9/20/2008 16:06:26 c0d2b77e3a84eda2e6cb38ec1396a280
    node4    9/20/2008 16:06:27 c0d2b77e3a84eda2e6cb38ec1396a280
4 entries were displayed.
```

---

## vserver services nis-domain create

Create a NIS domain configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services nis-domain create` command creates a configuration for an NIS domain. You can configure multiple NIS domains for a given Vserver, but only one NIS domain can be active on a Vserver at any given time. You can also configure more than one Vserver with the same NIS domain.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver on which the NIS domain configuration is created.

**-domain** <nis domain> - NIS Domain

Use this parameter to specify the NIS domain for which a configuration is created.

**-active** {true|false} - Active Domain

Use this parameter with the value `true` to specify that the NIS domain configuration is active when it is created. Use this parameter with the value `false` to specify that the NIS domain configuration is not active.

**-servers** <IP Address>, ... - NIS server

Use this parameter to specify the IP addresses of NIS servers used by the NIS domain configuration. Separate multiple IP addresses with commas.

### Examples

The following example creates an NIS domain configuration on the Vserver named `vs0`. The NIS domain is named `nisdomain`, is active upon creation, and uses an NIS server with the IP address `192.0.2.180`.

```
cluster1::> vserver services nis-domain create -vserver vs0 -domain nisdomain -  
active true -servers 192.0.2.180
```

---

## vserver services nis-domain delete

Delete a NIS domain configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services nis-domain delete` command deletes an NIS domain configuration.

Deleting an NIS domain configuration removes it permanently. To disable a configuration without deleting it, use the `vserver services nis-domain modify` command with the `-active false` parameter.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver from which the NIS domain configuration is deleted.

**-domain** <nis domain> - NIS Domain

Use this parameter to specify the NIS domain whose configuration is deleted.

### Examples

The following example deletes the configuration of an NIS domain named `testnisdomain` from a Vserver named `vs2`:

```
cluster1::> vserver services nis-domain delete -vserver vs2 -domain testnisdomain
```

### See Also

`vserver services nis-domain modify`



---

## vserver services nis-domain modify

Modify a NIS domain configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `vserver services nis-domain modify` command to modify the activity status and NIS server of an NIS domain configuration.

Use the `-active false` parameter to disable an NIS domain configuration without deleting it. To permanently remove a configuration, use the `vserver services nis-domain delete` command.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver whose NIS domain configuration is modified.

**-domain** <nis domain> - NIS Domain

Use this parameter to specify the NIS domain whose configuration is modified.

**[-active {true|false}]** - Active Domain

Use this parameter with the value `true` to specify that the NIS domain configuration is active. Use this parameter with the value `false` to specify that the NIS domain configuration is not active.

**[-servers <IP Address>, ...]** - NIS server

Use this parameter to specify the IP addresses of NIS servers used by the the NIS domain configuration. Separate multiple IP addresses with commas.

### Examples

The following example disables the configuration of an NIS domain named `nisdomain` on a Vserver named `vs0`:

```
cluster1::> vserver services nis-domain modify -vserver vs0 -domain nisdomain -  
active false
```

### See Also

---

vserver services nis-domain delete

---

## vserver services nis-domain show

Display NIS domain configurations

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services nis-domain show` command displays information about NIS domain configurations.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

Use this parameter to display information only about the NIS domain configurations of the Vservers you specify. Use this parameter with the `-domain` parameter to display information only about a particular NIS domain configuration on the Vserver you specify.

**[-domain <nis domain>]** - NIS Domain

Use this parameter to display information only about the NIS domain configurations that match the NIS domain name you specify. Use this parameter with the `-vserver` parameter to display information only about a particular NIS domain configuration on the Vserver you specify.

**[-active {true|false}]** - Active Domain

Use this parameter with the value `true` to display information only about the NIS domain configurations that are active. Use this parameter with the value `false` to display information only about the NIS domain configurations that are not active.

**[-servers <IP Address>, ...]** - NIS server

---

Use this parameter to display information only about the NIS domain configurations that use the NIS servers at the IP addresses you specify.

## Examples

The following example displays information about all NIS domain configurations:

```
cluster1::> vserver services nis-domain show
Vserver      Domain      Active NIS Server
-----
node1        nisdomain   true    192.0.2.180
node2        nisdomain   true    10.0.2.15
node2        nisdomain   false   192.0.2.180
node3        testnisdomain true    192.0.2.128, 192.0.2.180
4 entries were displayed.
```

---

## vserver services unix-group adduser

Add a user to a local UNIX group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services unix-group adduser` command adds a user to a local UNIX group.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver location of the local UNIX group to which the user is added.

**-name** <text> - Group Name

Use this parameter to specify the local UNIX group to which to add the user.

**-username** <text> - Name of User

Use this parameter to specify the user name to add to the local UNIX group.

### Examples

The following example adds a user named `tsmith` to a local UNIX group named `sales` on a Vserver named `vs0`:

```
cluster1::> vserver services unix-group adduser -vserver vs0 -name sales -  
username tsmith
```

## vserver services unix-group create

Create a local UNIX group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

---

The `vserver services unix-group create` command creates a local UNIX group on a Vserver. Use a local UNIX group for Windows-to-UNIX and UNIX-to-Windows group mappings.

## Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver on which to create the local UNIX group.

**-name** <text> - Group Name

Use this parameter to specify the name of the group to create.

**-id** <integer> - Group ID

Use this parameter to specify an ID number for the group.

## Examples

The following example creates a group named `sales` on a Vserver named `vs0`. The group has the ID 94.

```
cluster1::> vserver services unix-group create -vserver vs0 -name sales -id 94
```

## vserver services unix-group delete

Delete a local UNIX group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver services unix-group delete` command deletes a local UNIX group from a Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver location of the local UNIX group to delete.

**-name** <text> - Group Name

Use this parameter to specify the local UNIX group to delete.

## Examples

---

The following example deletes a local UNIX group named testgroup from a Vserver named vs0:

```
cluster1::> vserver services unix-group delete -vserver vs0 -name testgroup
```

## vserver services unix-group deluser

Delete a user from a local UNIX group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services unix-group deluser` command removes a user from a local UNIX group.

### Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver location of the local UNIX group from which the user is removed.

**-name** <text> - Group Name

Use this parameter to specify the local UNIX group from which to remove the user.

**-username** <text> - Name of User

Use this parameter to specify the user name to remove from the local UNIX group.

### Examples

The following example removes a user named testuser from a local UNIX group named sales on a Vserver named vs0:

```
cluster1::> vserver services unix-group deluser -vserver vs0 -name eng -username  
testuser
```

## vserver services unix-group load-from-uri

Load one or more local UNIX groups from a URI

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

---

## Description

The `vserver services unix-group load-from-uri` command loads UNIX groups from a universal resource identifier (URI). The URI must contain group information in the UNIX `/etc/group` format:

`group_name:password:group_ID:comma_separated_list_of_users`

The command discards the value of the password field.

## Parameters

**-vserver** <vserver> - Vserver

Use this parameter to specify the Vserver on which to locate the local UNIX groups.

**-uri** {(ftp|http):||(hostname|IPv4 Address|['IPv6 Address'])...} - URI to Load From

Use this parameter to specify the URI from which the command loads group information.

**[-overwrite {true|false}]** - Overwrite Entries

Use this parameter with the value `true` to specify that group information loaded from the URI should overwrite existing group information. The default value is `false`, specifying that group information loaded from the URI should not overwrite existing group information.

## Examples

The following example loads group information from the URI `ftp://ftp.example.com/groups` onto a Vserver named `vs0`:

```
cluster1:> vserver services unix-group load-from-uri -vserver vs0 -uri ftp://  
ftp.example.com/groups
```

## vserver services unix-group modify

Modify a local UNIX group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

Use the `vserver services unix-group modify` command to modify a local UNIX group's group ID.



---

## Parameters

**-vserver** <vserver name> - Vserver

Use this parameter to specify the Vserver location of the local UNIX group to modify.

**-name** <text> - Group Name

Use this parameter to specify the name of the group to modify.

**[-id <integer>]** - Group ID

Use this parameter to specify an ID number for the group.

## Examples

The following example changes a local UNIX group named sales on a Vserver named vs0 to have the group ID 100:

```
cluster1::> vsserver services unix-group modify -vserver vs0 -group sales -id 100
```

## vserver services unix-group show

Display local UNIX groups

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vsserver services unix-group show` command displays information about local UNIX groups.

## Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-members]**

Use this parameter to display the list of users in each local UNIX group.

| **[-instance]** }

---

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**`[-vserver <vserver name>]`** - Vserver

Use this parameter with the `-name` parameter to display information only about the local UNIX group you specify. Use this parameter without `-name` to display information only about the local UNIX groups that are located on the specified Vserver.

**`[-name <text>]`** - Group Name

Use this parameter with the `-vserver` parameter to display information only about the local UNIX group you specify. Use this parameter without `-vserver` to display information only about the local UNIX groups that match the name you specify.

**`[-id <integer>]`** - Group ID

Use this parameter to display information only about the local UNIX group that has the ID you specify.

**`[-users <text>, ...]`** - Users

Use this parameter to display information only about the local UNIX groups that include the user names you specify.

## Examples

The following example displays information about all local UNIX groups, including lists of their users:

```
cluster1::> vserver services unix-group show -members
Vserver      Name      ID
vs0          dev        44
Users: admin, jdoe, tsmith
vs0          sales     12
Users: admin, guest, pjones
vs1          testgroup  13
Users: admin, root, testuser
vs1          users     100
Users: admin, jdoe, pjones, tsmith
```

---

## vserver services unix-user create

Create a local UNIX user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver services unix-user create` command creates a local UNIX user on a Vserver. You can use local UNIX users for Windows-to-UNIX and UNIX-to-Windows name mappings.

### Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which you want to create the local unix user.

**-user** <text> - User Name

This parameter specifies the user account that you want to create.

**-id** <integer> - User ID

This parameter specifies an ID number for the user.

**-primary-gid** <integer> - Primary Group ID

This parameter specifies the ID number of the user's primary group.

**[-full-name** <text>] - User's Full Name

This parameter specifies the user's full name.

### Examples

The following example creates a local UNIX user named tsmith on a Vserver named vs0. The user has the ID 4219 and the primary group ID 100. The user's full name is Tom Smith.

```
vs1::> vserver services unix-user create -vserver vs0 -user tsmith -id 4219 -  
primary-gid 100 -full-name "Tom Smith"
```

## vserver services unix-user delete

---

Delete a local UNIX user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver services unix-user delete` command deletes a local UNIX user from a Vserver.

## Parameters

**-vserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the local UNIX user is located.

**-user** <text> - User Name

This parameter specifies the user that you want to delete.

## Examples

The following example deletes a local UNIX user named `testuser` from a Vserver named `vs0`:

```
vs1::> vserver services unix-user delete -vserver vs0 -user testuser
```

## vserver services unix-user load-from-uri

Load one or more local UNIX users from a URI

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver services unix-user load-from-uri` command loads one or more UNIX users from a universal resource identifier (URI). The URI must contain user information in the UNIX `/etc/passwd` format: `user_name: password: user_ID: group_ID: full_name`. The command discards the value of the password field and of the fields after the `full_name` field ( `home_directory` and `shell`).

## Parameters

**-vserver** <vserver> - Vserver

---

This specifies the Vserver on which the local UNIX user or users are to be located.

**-uri** {(ftp|http)://[(hostname|IPv4 Address|'IPv6 Address')]...} - URI to Load From

This specifies the URI from which user information is to be loaded.

**-overwrite** {true|false} - Overwrite Entries

This optionally specifies whether user information from the URI overwrites existing user information. The default setting is `false`.

## Examples

The following example loads user information from the URI `ftp://ftp.example.com/users` onto a Vserver named `vs0`:

```
node::> vsserver services unix-user load-from-uri -vsserver vs0 -uri ftp://  
ftp.example.com/users
```

## vserver services unix-user modify

Modify a local UNIX user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vsserver services unix-user modify` command modifies a local UNIX user's ID, primary group ID, or full name.

## Parameters

**-vsserver** <vserver name> - Vserver

This parameter specifies the Vserver on which the local UNIX user is located.

**-user** <text> - User Name

This parameter specifies the user account that you want to modify.

**[-id <integer>]** - User ID

This optional parameter specifies an ID number for the user.

**[-primary-gid <integer>]** - Primary Group ID

This optional parameter specifies the ID number of the user's primary group.

**[-full-name <text>]** - User's Full Name

---

This optional parameter specifies the user's full name.

## Examples

The following example modifies the local UNIX user named pjones on a Vserver named vs0. The user's primary group ID is changed to 100 and the user's full name is Peter Jones.

```
vs1::> vsserver services unix-user modify -vsserver vs0 -user pjones -primary-gid
100 -full-name "Peter Jones"
```

## vserver services unix-user show

Display local UNIX users

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vsserver services unix-user show` command displays information about local UNIX users. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all local UNIX users:

- Vserver name
- User name
- User ID
- Primary group ID
- Full name

## Parameters

{ [-**fields** <fieldname>, ...]

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| [-**instance** ] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

[-**vserver** <vserver name>] - Vserver

---

If you specify this parameter and the `-user` parameter, the command displays information only about the specified local UNIX user. If you specify this parameter by itself, the command displays information only about the local UNIX user or users that are located on the specified Vserver.

**`[-user <text>]`** - User Name

If you specify this parameter and the `-vserver` parameter, the command displays information only about the specified local UNIX user. If you specify this parameter by itself, the command displays information only about the local UNIX user or users that have the specified name.

**`[-id <integer>]`** - User ID

If you specify this parameter, the command displays information only about the local UNIX user that has the specified ID.

**`[-primary-gid <integer>]`** - Primary Group ID

If you specify this parameter, the command displays information only about the local UNIX user or users that have the specified primary group ID.

**`[-full-name <text>]`** - User's Full Name

If you specify this parameter, the command displays information only about the local UNIX user or users that match the specified name.

## Examples

The following example displays information about all local UNIX users:

```
vs1::> vsserver services unix-user show
Vserver      User      User      Group      Full
              Name      ID        ID          Name
-----
vs0          admin      100       100        administrator
vs0          guest     1000      100         guest
vs0          jdoe      4673      100        Jane Doe
vs0          monitor   2000      100        monitor
vs0          pjones    4236      100        Peter Jones
vs0          root      10        100         root
vs0          tsmith    3289      100         Tom Smith
```

---

## vserver services web modify

Modify the configuration of web services

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command modifies the availability of the web services on Vservers. Only the services that are installed on every node in the cluster can be configured on Vservers whose type is not 'node'. Enabled services must include authorization configuration in the `vserver services web access` command for the services to be externally available.

### Parameters

**-vserver** <vserver name> - Vserver

Identifies a Vserver for hosting a specific web service.

**-name** <text> - Service Name

Identifies the name of the web service.

**[-enabled {true|false}]** - Enabled

Defines the availability of a service on the Vserver. Disabled services are not accessible through the Vserver's network interfaces. This parameter's default value is dependent on the service. In general, services that provide commonly used features are enabled by default.

**[-ssl-only {true|false}]** - SSL Only

Defines the encryption enforcement policy for a service on the Vserver. Services for which this parameter is set to true support SSL only and cannot be used over unencrypted HTTP. The default for this value is 'false'.

### Examples

The following command sets access to the web port to SSL only:

```
cluster1::> vserver services web modify -vserver vs1 -name portal -ssl-only true
```

### See Also



---

system services web packages   vserver services web access

---

## vserver services web show

Display the current configuration of web services

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the availability of the web services on Vservers. Only the services that are installed on every node in the cluster can be configured on Vservers whose type is not 'node'. Enabled services must include authorization configuration in the `vserver services web access` command for the services to be externally available.

### Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Identifies a Vserver for hosting a specific web service.

[-name <text>] - Service Name

Identifies the name of the web service.

[-type <vserver type>] - Type of Vserver

Identifies the type of Vserver on which the service is hosted.

[-version <text>] - Version of Web Service

Defines the version number of the service in the format of major.minor.patch.

[-description <text>] - Description of Web Service

Provides a short description of the web service.

---

**[-long-description <text>]** - Long Description of Web Service

Provides a long description of the web service.

**[-requires <requirement>, ...]** - Service Requirements

Defines the list of requirements that must be met for the service to be successfully executed. Requirements are defined as a service name, a comparison operator (<=>), and a version number.

**[-default-roles <text>, ...]** - Default Authorized Roles

Defines the roles that are automatically granted access to the service in the `vserver services web access show` configuration.

**[-enabled {true|false}]** - Enabled

Defines the availability of a service on the Vserver. Disabled services are not accessible through the Vserver's network interfaces. This parameter's default value is dependent on the service. In general, services that provide commonly used features are enabled by default.

**[-ssl-only {true|false}]** - SSL Only

Defines the encryption enforcement policy for a service on the Vserver. Services for which this parameter is set to true support SSL only and cannot be used over unencrypted HTTP. The default for this value is 'false'.

## Examples

This example displays the availability of the web services on the Vservers.

```
clus01::vserver services web> show
Vserver      Type      Service Name      Description      Enabled
-----
clus01       admin     cem               OBSOLETE         true
clus01       admin     ontapi            Remote Administrative API   true
clus01       admin     portal            Data ONTAP Web Services    true
n6070-8      node     cem               OBSOLETE         true
n6070-8      node     ontapi            Remote Administrative API   true
n6070-8      node     portal            Data ONTAP Web Services    true
n6070-8      node     spi              Service Processor           false
n6070-8      node     supdiag           Infrastructure Support Diagnostics true
n6070-9      node     cem               OBSOLETE         true
n6070-9      node     ontapi            Remote Administrative API   true
n6070-9      node     portal            Data ONTAP Web Services    true
n6070-9      node     spi              Service Processor           false
n6070-9      node     supdiag           Infrastructure Support Diagnostics false
13 entries were displayed.
```

## See Also

---

vserver services web access show    system services web packages  
vserver services web access

---

## vserver services web access create

Authorize a new role for web service access

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command authorizes roles to access the Vserver's web services. For the user to access services that require authentication, the user's roles, as defined by `security login show`, must be included in this configuration.

Note:

Node Vserver services are authorized with the data Vserver's roles.

### Parameters

**-vserver** <vserver name> - Vserver

Identifies a Vserver for hosting a specific web service.

**-name** <text> - Service Name

Identifies the name of the web service.

**-role** <text> - Role Name

Identifies the new role to be authorized for this service.

### Examples

The following example authorizes the role auditor - created previously - for the web service:

```
cluster1::> vserver services web access create -name ontapi -role auditor
```

### See Also

`security login show`

---

## vserver services web access delete

Remove role authorization for web service access

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command removes the authorization of a role from the Vserver's web services. A service for which no roles are defined has a single role of 'none' automatically displayed in this configuration.

Note:

Node Vserver services are authorized with the data Vserver's roles.

### Parameters

**-vserver** <vserver name> - Vserver

Identifies a Vserver for hosting a specific web service.

**-name** <text> - Service Name

Identifies the name of the web service.

**-role** <text> - Role Name

Identifies the role whose authorization is to be removed. You cannot remove the authorization of the role 'none'. Use `vserver services web access create` to authorize access for the role.

### Examples

The following example removes authorization for the role auditor for the web service:

```
cluster1::> vserver services web access delete -name ontapi -role auditor
```

### See Also

`vserver services web access create`

---

## vserver services web access show

Display web service authorization for user roles

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command displays the roles that are authorized to access the Vserver's web services. For the user to access services that require authentication, the user's roles, as defined by `security login show`, must be included in this configuration.

Note:

Node Vserver services are authorized with the data Vserver's roles.

### Parameters

{ **[-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| **[-instance ]** }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>]** - Vserver

Identifies a Vserver for hosting a specific web service.

**[-name <text>]** - Service Name

Identifies the name of the web service.

**[-role <text>]** - Role Name

Identifies a role assigned for accessing the service. A service without any authorizations has a role of 'none' assigned to it automatically.

**[-type <vserver type>]** - Type of Vserver

Identifies the type of Vserver on which the service is hosted.

---

# Examples

The following example displays the roles that are authorized to access the web services.

```
clus01::vserver services web access> show
Vserver      Type      Service Name  Role
-----
clus01       admin     cem           none
clus01       admin     ontapi        readonly
clus01       admin     portal        none
clus01       admin     spi           none
clus01       admin     supdiag       none
vs0          cluster   ontapi        admin
6 entries were displayed.

clus01::vserver services web access>
```

## See Also

security login show



---

## vserver smtape break

Make a restored volume read-write

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command breaks the relationship between the tape backup of a volume and a restored volume, changing the restored volume from read-only to read/write.

### Parameters

**-vserver** <vserver name> - Vserver Name

Use this parameter to specify the Vserver name on which the volume is located.

**-volume** <volume name> - Volume Name

Use this parameter to specify the name of the read-only volume that needs to be changed into a read/writeable volume after an smtape restore.

### Examples

Make the read-only volume datavol on Vserver vserver0 writeable after a restore.

```
clus1:> vserver smtape break -vserver vserver0 -volume datavol
[Job 84] Job succeeded: SnapMirror Break Succeeded
```

### See Also

system smtape backup   system smtape restore