vserver commands

ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-991/vserver-add-aggregates.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

vserver commands . . . 1
- vserver add-aggregates . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- vserver add-protocols . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 2
- vserver context . . . 2
  - Description . . . 2
  - Parameters . . . 2
  - Examples . . . 2
  - Related Links . . . 2
- vserver create . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 4
  - Related Links . . . 5
- vserver delete . . . 5
  - Description . . . 5
  - Parameters . . . 5
  - Examples . . . 6
  - Related Links . . . 6
- vserver modify . . . 6
  - Description . . . 6
  - Parameters . . . 6
  - Examples . . . 8
- vserver prepare-for-revert . . . 8
  - Description . . . 8
  - Examples . . . 8
- vserver remove-aggregates . . . 8
  - Description . . . 8
  - Parameters . . . 8
  - Examples . . . 8
- vserver remove-protocols . . . 9
  - Description . . . 9
  - Parameters . . . 9
  - Examples . . . 9
- vserver rename . . . 9
  - Description . . . 9
  - Parameters . . . 9
  - Examples . . . 10

vserver restamp-msid . . . 10
Description . . . 10
Parameters . . . 11
Examples . . . 11
Related Links . . . 11
vserver show-aggregates . . . 11
Description . . . 11
Parameters . . . 11
Examples . . . 12
vserver show-protocols . . . 12
Description . . . 12
Parameters . . . 12
Examples . . . 12
vserver show . . . 13
Description . . . 13
Parameters . . . 13
Examples . . . 17
vserver start . . . 17
Description . . . 18
Parameters . . . 18
Examples . . . 18
vserver stop . . . 18
Description . . . 18
Parameters . . . 18
Examples . . . 19
vserver unlock . . . 19
Description . . . 19
Parameters . . . 19
Examples . . . 19
vserver active-directory commands . . . 19
vserver active-directory create . . . 19
vserver active-directory delete . . . 22
vserver active-directory modify . . . 22
vserver active-directory password-change . . . 23
vserver active-directory password-reset . . . 23
vserver active-directory show . . . 24
vserver audit commands . . . 26
vserver audit create . . . 26
vserver audit delete . . . 29
vserver audit disable . . . 29
vserver audit enable . . . 30
vserver audit modify . . . 30
vserver audit prepare-to-downgrade . . . 32
vserver audit rotate-log . . . 33
vserver audit show . . . 33

vserver audit audit-log-redirect create . . . 36
vserver audit audit-log-redirect delete . . . 37
vserver audit audit-log-redirect modify . . . 37
vserver audit audit-log-redirect show . . . 38
vserver check commands . . . 38
vserver check lif-multitenancy run . . . 38
vserver check lif-multitenancy show-results . . . 40
vserver check lif-multitenancy show . . . 42
vserver cifs commands . . . 43
vserver cifs add-netbios-aliases . . . 43
vserver cifs check . . . 45
vserver cifs create . . . 47
vserver cifs delete . . . 49
vserver cifs modify . . . 50
vserver cifs nbtstat . . . 53
vserver cifs prepare-to-downgrade . . . 56
vserver cifs remove-netbios-aliases . . . 57
vserver cifs repair-modify . . . 58
vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade . . . 59
vserver cifs show . . . 60
vserver cifs start . . . 62
vserver cifs stop . . . 63
vserver cifs branchcache create . . . 63
vserver cifs branchcache delete . . . 65
vserver cifs branchcache hash-create . . . 65
vserver cifs branchcache hash-flush . . . 66
vserver cifs branchcache modify . . . 67
vserver cifs branchcache show . . . 68
vserver cifs cache name-to-sid delete-all . . . 70
vserver cifs cache name-to-sid delete . . . 71
vserver cifs cache name-to-sid show . . . 71
vserver cifs cache settings modify . . . 73
vserver cifs cache settings show . . . 74
vserver cifs cache sid-to-name delete-all . . . 75
vserver cifs cache sid-to-name delete . . . 76
vserver cifs cache sid-to-name show . . . 76
vserver cifs character-mapping create . . . 78
vserver cifs character-mapping delete . . . 79
vserver cifs character-mapping modify . . . 79
vserver cifs character-mapping show . . . 80
vserver cifs connection show . . . 81
vserver cifs domain discovered-servers reset-servers . . . 83
vserver cifs domain discovered-servers show . . . 83
vserver cifs domain discovered-servers discovery-mode modify . . . 85
vserver cifs domain discovered-servers discovery-mode show . . . 86

vserver cifs domain name-mapping-search add . . . 86
vserver cifs domain name-mapping-search modify . . . 87
vserver cifs domain name-mapping-search remove . . . 88
vserver cifs domain name-mapping-search show . . . 88
vserver cifs domain password change . . . 89
vserver cifs domain password reset . . . 89
vserver cifs domain password schedule modify . . . 90
vserver cifs domain password schedule show . . . 91
vserver cifs domain preferred-dc add . . . 93
vserver cifs domain preferred-dc check . . . 94
vserver cifs domain preferred-dc remove . . . 95
vserver cifs domain preferred-dc show . . . 96
vserver cifs domain trusts rediscover . . . 96
vserver cifs domain trusts show . . . 97
vserver cifs group-policy modify . . . 98
vserver cifs group-policy show-applied . . . 99
vserver cifs group-policy show-defined . . . 101
vserver cifs group-policy show . . . 103
vserver cifs group-policy update . . . 104
vserver cifs group-policy central-access-policy show-applied . . . 105
vserver cifs group-policy central-access-policy show-defined . . . 107
vserver cifs group-policy central-access-rule show-applied . . . 108
vserver cifs group-policy central-access-rule show-defined . . . 110
vserver cifs group-policy restricted-group show-applied . . . 112
vserver cifs group-policy restricted-group show-defined . . . 114
vserver cifs home-directory modify . . . 116
vserver cifs home-directory show-user . . . 117
vserver cifs home-directory show . . . 119
vserver cifs home-directory search-path add . . . 120
vserver cifs home-directory search-path remove . . . 120
vserver cifs home-directory search-path reorder . . . 121
vserver cifs home-directory search-path show . . . 121
vserver cifs options modify . . . 122
vserver cifs options show . . . 128
vserver cifs security modify . . . 135
vserver cifs security show . . . 138
vserver cifs session close . . . 142
vserver cifs session show . . . 144
vserver cifs session file close . . . 149
vserver cifs session file show . . . 150
vserver cifs share create . . . 154
vserver cifs share delete . . . 158
vserver cifs share modify . . . 159
vserver cifs share show . . . 162
vserver cifs share access-control create . . . 166

vserver cifs share access-control delete . . . 167
vserver cifs share access-control modify . . . 168
vserver cifs share access-control show . . . 169
vserver cifs share properties add . . . 170
vserver cifs share properties remove . . . 172
vserver cifs share properties show . . . 173
vserver cifs superuser create . . . 175
vserver cifs superuser delete . . . 176
vserver cifs superuser show . . . 176
vserver cifs symlink create . . . 177
vserver cifs symlink delete . . . 179
vserver cifs symlink modify . . . 179
vserver cifs symlink show . . . 181
vserver cifs users-and-groups remove-stale-records . . . 182
vserver cifs users-and-groups update-names . . . 183
vserver cifs users-and-groups local-group add-members . . . 184
vserver cifs users-and-groups local-group create . . . 185
vserver cifs users-and-groups local-group delete . . . 186
vserver cifs users-and-groups local-group modify . . . 186
vserver cifs users-and-groups local-group remove-members . . . 187
vserver cifs users-and-groups local-group rename . . . 187
vserver cifs users-and-groups local-group show-members . . . 188
vserver cifs users-and-groups local-group show . . . 189
vserver cifs users-and-groups local-user create . . . 190
vserver cifs users-and-groups local-user delete . . . 192
vserver cifs users-and-groups local-user modify . . . 192
vserver cifs users-and-groups local-user rename . . . 193
vserver cifs users-and-groups local-user set-password . . . 194
vserver cifs users-and-groups local-user show-membership . . . 195
vserver cifs users-and-groups local-user show . . . 196
vserver cifs users-and-groups privilege add-privilege . . . 197
vserver cifs users-and-groups privilege remove-privilege . . . 198
vserver cifs users-and-groups privilege reset-privilege . . . 199
vserver cifs users-and-groups privilege show . . . 200
vserver config-replication commands . . . 201
vserver config-replication pause . . . 201
vserver config-replication resume . . . 202
vserver config-replication show . . . 202
vserver export-policy commands . . . 203
vserver export-policy check-access . . . 203
vserver export-policy copy . . . 207
vserver export-policy create . . . 208
vserver export-policy delete . . . 208
vserver export-policy rename . . . 209
vserver export-policy show . . . 209

vserver export-policy access-cache flush . . . 210
vserver export-policy access-cache show-rules . . . 212
vserver export-policy access-cache show . . . 216
vserver export-policy access-cache config modify-all-vservers . . . 219
vserver export-policy access-cache config modify . . . 220
vserver export-policy access-cache config show-all-vservers . . . 221
vserver export-policy access-cache config show . . . 222
vserver export-policy cache flush . . . 223
vserver export-policy config-checker show . . . 224
vserver export-policy config-checker start . . . 226
vserver export-policy config-checker stop . . . 226
vserver export-policy config-checker rule delete . . . 227
vserver export-policy config-checker rule show . . . 228
vserver export-policy netgroup check-membership . . . 230
vserver export-policy netgroup cache show . . . 231
vserver export-policy netgroup queue show . . . 233
vserver export-policy rule add-clientmatches . . . 235
vserver export-policy rule create . . . 236
vserver export-policy rule delete . . . 241
vserver export-policy rule modify . . . 242
vserver export-policy rule remove-clientmatches . . . 247
vserver export-policy rule setindex . . . 248
vserver export-policy rule show . . . 249
vserver fcp commands . . . 254
vserver fcp create . . . 254
vserver fcp delete . . . 255
vserver fcp modify . . . 256
vserver fcp show . . . 257
vserver fcp start . . . 258
vserver fcp stop . . . 258
vserver fcp initiator show . . . 259
vserver fcp interface show . . . 260
vserver fcp nameserver show . . . 262
vserver fcp ping-igroup show . . . 264
vserver fcp ping-initiator show . . . 265
vserver fcp portname set . . . 266
vserver fcp portname show . . . 267
vserver fcp topology show . . . 268
vserver fcp wwn blacklist show . . . 270
vserver fcp wwpn-alias remove . . . 271
vserver fcp wwpn-alias set . . . 272
vserver fcp wwpn-alias show . . . 273
vserver fpolicy commands . . . 274
vserver fpolicy disable . . . 274
vserver fpolicy enable . . . 275

vserver fpolicy engine-connect . . . 276
vserver fpolicy engine-disconnect . . . 278
vserver fpolicy show-enabled . . . 278
vserver fpolicy show-engine . . . 280
vserver fpolicy show-passthrough-read-connection . . . 282
vserver fpolicy show . . . 285
vserver fpolicy policy create . . . 286
vserver fpolicy policy delete . . . 288
vserver fpolicy policy modify . . . 288
vserver fpolicy policy show . . . 290
vserver fpolicy policy event create . . . 292
vserver fpolicy policy event delete . . . 298
vserver fpolicy policy event modify . . . 299
vserver fpolicy policy event show . . . 305
vserver fpolicy policy external-engine create . . . 307
vserver fpolicy policy external-engine delete . . . 311
vserver fpolicy policy external-engine modify . . . 312
vserver fpolicy policy external-engine show . . . 316
vserver fpolicy policy scope create . . . 320
vserver fpolicy policy scope delete . . . 323
vserver fpolicy policy scope modify . . . 324
vserver fpolicy policy scope show . . . 326
vserver http-proxy commands . . . 329
vserver http-proxy create . . . 329
vserver http-proxy delete . . . 331
vserver http-proxy modify . . . 331
vserver http-proxy show . . . 332
vserver iscsi commands . . . 334
vserver iscsi create . . . 334
vserver iscsi delete . . . 335
vserver iscsi modify . . . 335
vserver iscsi show . . . 337
vserver iscsi start . . . 340
vserver iscsi stop . . . 340
vserver iscsi command show . . . 341
vserver iscsi connection show . . . 343
vserver iscsi connection shutdown . . . 345
vserver iscsi initiator show . . . 346
vserver iscsi interface disable . . . 347
vserver iscsi interface enable . . . 348
vserver iscsi interface modify . . . 348
vserver iscsi interface show . . . 349
vserver iscsi interface accesslist add . . . 351
vserver iscsi interface accesslist remove . . . 353
vserver iscsi interface accesslist show . . . 353

vserver iscsi isns create . . . 354
vserver iscsi isns delete . . . 355
vserver iscsi isns modify . . . 356
vserver iscsi isns show . . . 357
vserver iscsi isns start . . . 358
vserver iscsi isns stop . . . 359
vserver iscsi isns update . . . 359
vserver iscsi security add-initator-address-ranges . . . 360
vserver iscsi security create . . . 360
vserver iscsi security default . . . 362
vserver iscsi security delete . . . 363
vserver iscsi security modify . . . 364
vserver iscsi security prepare-to-downgrade . . . 365
vserver iscsi security remove-initator-address-ranges . . . 365
vserver iscsi security show . . . 366
vserver iscsi session show . . . 369
vserver iscsi session shutdown . . . 372
vserver iscsi session parameter show . . . 373
vserver locks commands . . . 376
vserver locks break . . . 376
vserver locks show . . . 378
vserver name-mapping commands . . . 391
vserver name-mapping create . . . 391
vserver name-mapping delete . . . 392
vserver name-mapping insert . . . 393
vserver name-mapping modify . . . 394
vserver name-mapping refresh-hostname-ip . . . 395
vserver name-mapping show . . . 396
vserver name-mapping swap . . . 398
vserver nfs commands . . . 398
vserver nfs create . . . 398
vserver nfs delete . . . 407
vserver nfs modify . . . 407
vserver nfs off . . . 416
vserver nfs on . . . 416
vserver nfs prepare-for-v3-ms-dos-client-downgrade . . . 417
vserver nfs prepare-to-downgrade . . . 417
vserver nfs show . . . 418
vserver nfs start . . . 426
vserver nfs status . . . 427
vserver nfs stop . . . 427
vserver nfs connected-clients show . . . 428
vserver nfs credentials count . . . 429
vserver nfs credentials flush . . . 430
vserver nfs credentials show . . . 431

vserver nfs kerberos interface disable . . . 433
vserver nfs kerberos interface enable . . . 434
vserver nfs kerberos interface modify . . . 435
vserver nfs kerberos interface show . . . 436
vserver nfs kerberos realm create . . . 438
vserver nfs kerberos realm delete . . . 439
vserver nfs kerberos realm modify . . . 440
vserver nfs kerberos realm show . . . 442
vserver nfs pnfs devices create . . . 444
vserver nfs pnfs devices delete . . . 445
vserver nfs pnfs devices show . . . 445
vserver nfs pnfs devices cache show . . . 447
vserver nfs pnfs devices mappings show . . . 448
vserver nvme commands . . . 449
vserver nvme create . . . 449
vserver nvme delete . . . 450
vserver nvme modify . . . 451
vserver nvme show-interface . . . 451
vserver nvme show . . . 453
vserver nvme feature show . . . 453
vserver nvme namespace create . . . 454
vserver nvme namespace delete . . . 455
vserver nvme namespace modify . . . 456
vserver nvme namespace show . . . 456
vserver nvme subsystem create . . . 459
vserver nvme subsystem delete . . . 460
vserver nvme subsystem modify . . . 461
vserver nvme subsystem show . . . 461
vserver nvme subsystem controller show . . . 463
vserver nvme subsystem host add . . . 464
vserver nvme subsystem host remove . . . 465
vserver nvme subsystem host show . . . 466
vserver nvme subsystem map add . . . 467
vserver nvme subsystem map remove . . . 468
vserver nvme subsystem map show . . . 468
vserver object-store-server commands . . . 469
vserver object-store-server create . . . 469
vserver object-store-server delete . . . 470
vserver object-store-server modify . . . 471
vserver object-store-server show . . . 472
vserver object-store-server bucket create . . . 474
vserver object-store-server bucket delete . . . 475
vserver object-store-server bucket evict-remote-cached-objects . . . 475
vserver object-store-server bucket modify . . . 476
vserver object-store-server bucket show . . . 476

vserver object-store-server bucket policy-statement-condition create 478
vserver object-store-server bucket policy-statement-condition delete 480
vserver object-store-server bucket policy-statement-condition modify 481
vserver object-store-server bucket policy-statement-condition show 482
vserver object-store-server bucket policy statement create 483
vserver object-store-server bucket policy statement delete 484
vserver object-store-server bucket policy statement modify 485
vserver object-store-server bucket policy statement show 486
vserver object-store-server group create 488
vserver object-store-server group delete 489
vserver object-store-server group modify 489
vserver object-store-server group show 490
vserver object-store-server policy create 492
vserver object-store-server policy delete 492
vserver object-store-server policy modify 493
vserver object-store-server policy show 493
vserver object-store-server policy statement create 495
vserver object-store-server policy statement delete 496
vserver object-store-server policy statement modify 496
vserver object-store-server policy statement show 497
vserver object-store-server user create 499
vserver object-store-server user delete 500
vserver object-store-server user modify 500
vserver object-store-server user regenerate-keys 501
vserver object-store-server user show 501
vserver peer commands 504
vserver peer accept 504
vserver peer create 505
vserver peer delete 508
vserver peer modify-local-name 509
vserver peer modify 510
vserver peer reject 510
vserver peer repair-peer-name 511
vserver peer resume 511
vserver peer show-all 512
vserver peer show 514
vserver peer suspend 517
vserver peer permission create 517
vserver peer permission delete 518
vserver peer permission modify 519
vserver peer permission show 520
vserver peer transition create 521
vserver peer transition delete 521
vserver peer transition modify 522
vserver peer transition show 523

vserver san commands . . . 524
vserver san prepare-to-downgrade . . . 524
vserver security commands . . . 524
vserver security file-directory apply . . . 524
vserver security file-directory remove-slag . . . 526
vserver security file-directory show-effective-permissions . . . 528
vserver security file-directory show . . . 530
vserver security file-directory job show . . . 536
vserver security file-directory ntfs create . . . 539
vserver security file-directory ntfs delete . . . 541
vserver security file-directory ntfs modify . . . 542
vserver security file-directory ntfs show . . . 543
vserver security file-directory ntfs dacl add . . . 544
vserver security file-directory ntfs dacl modify . . . 547
vserver security file-directory ntfs dacl remove . . . 550
vserver security file-directory ntfs dacl show . . . 551
vserver security file-directory ntfs sacl add . . . 554
vserver security file-directory ntfs sacl modify . . . 557
vserver security file-directory ntfs sacl remove . . . 560
vserver security file-directory ntfs sacl show . . . 561
vserver security file-directory policy create . . . 564
vserver security file-directory policy delete . . . 565
vserver security file-directory policy show . . . 565
vserver security file-directory policy task add . . . 566
vserver security file-directory policy task modify . . . 569
vserver security file-directory policy task remove . . . 571
vserver security file-directory policy task show . . . 572
vserver security trace filter create . . . 573
vserver security trace filter delete . . . 575
vserver security trace filter modify . . . 576
vserver security trace filter show . . . 578
vserver security trace trace-result delete . . . 580
vserver security trace trace-result show . . . 581
vserver services commands . . . 590
vserver services access-check authentication get-claim-name . . . 590
vserver services access-check authentication get-dc-info . . . 591
vserver services access-check authentication login-cifs . . . 592
vserver services access-check authentication ontap-admin-login-cifs . . . 593
vserver services access-check authentication show-creds . . . 594
vserver services access-check authentication show-ontap-admin-unix-creds . . . 598
vserver services access-check authentication sid-to-uid . . . 599
vserver services access-check authentication sid-to-unix-name . . . 600
vserver services access-check authentication translate . . . 600
vserver services access-check authentication uid-to-sid . . . 601
vserver services access-check dns forward-lookup . . . 602

vserver services access-check dns srv-lookup . . . 603
vserver services access-check name-mapping show . . . 604
vserver services access-check server-discovery reset . . . 605
vserver services access-check server-discovery show-host . . . 605
vserver services access-check server-discovery show-site . . . 606
vserver services access-check server-discovery test . . . 607
vserver services name-service cache group-membership delete-all . . . 607
vserver services name-service cache group-membership delete . . . 608
vserver services name-service cache group-membership show . . . 609
vserver services name-service cache group-membership settings modify . . . 610
vserver services name-service cache group-membership settings show . . . 611
vserver services name-service cache hosts forward-lookup delete-all . . . 612
vserver services name-service cache hosts forward-lookup delete . . . 612
vserver services name-service cache hosts forward-lookup show . . . 613
vserver services name-service cache hosts reverse-lookup delete-all . . . 615
vserver services name-service cache hosts reverse-lookup delete . . . 615
vserver services name-service cache hosts reverse-lookup show . . . 616
vserver services name-service cache hosts settings modify . . . 618
vserver services name-service cache hosts settings show . . . 619
vserver services name-service cache netgroups ip-to-netgroup delete-all . . . 620
vserver services name-service cache netgroups ip-to-netgroup delete . . . 621
vserver services name-service cache netgroups ip-to-netgroup show . . . 621
vserver services name-service cache netgroups members delete-all . . . 622
vserver services name-service cache netgroups members delete . . . 623
vserver services name-service cache netgroups members show . . . 623
vserver services name-service cache netgroups settings modify . . . 625
vserver services name-service cache netgroups settings show . . . 626
vserver services name-service cache settings modify . . . 627
vserver services name-service cache settings show . . . 627
vserver services name-service cache unix-group group-by-gid delete-all . . . 628
vserver services name-service cache unix-group group-by-gid delete . . . 628
vserver services name-service cache unix-group group-by-gid show . . . 629
vserver services name-service cache unix-group group-by-name delete-all . . . 630
vserver services name-service cache unix-group group-by-name delete . . . 631
vserver services name-service cache unix-group group-by-name show . . . 631
vserver services name-service cache unix-group settings modify . . . 632
vserver services name-service cache unix-group settings show . . . 633
vserver services name-service cache unix-user settings modify . . . 635
vserver services name-service cache unix-user settings show . . . 636
vserver services name-service cache unix-user user-by-id delete-all . . . 637
vserver services name-service cache unix-user user-by-id delete . . . 638
vserver services name-service cache unix-user user-by-id show . . . 638
vserver services name-service cache unix-user user-by-name delete-all . . . 640
vserver services name-service cache unix-user user-by-name delete . . . 640
vserver services name-service cache unix-user user-by-name show . . . 641

vserver services name-service dns check . . . 642
vserver services name-service dns create . . . 643
vserver services name-service dns delete . . . 644
vserver services name-service dns modify . . . 645
vserver services name-service dns show . . . 647
vserver services name-service dns dynamic-update modify . . . 648
vserver services name-service dns dynamic-update prepare-to-downgrade . . . 649
vserver services name-service dns dynamic-update show . . . 650
vserver services name-service dns dynamic-update record add . . . 651
vserver services name-service dns dynamic-update record delete . . . 651
vserver services name-service dns hosts create . . . 652
vserver services name-service dns hosts delete . . . 653
vserver services name-service dns hosts modify . . . 654
vserver services name-service dns hosts show . . . 655
vserver services name-service getxxbyyy getaddrinfo . . . 656
vserver services name-service getxxbyyy getgrbygid . . . 657
vserver services name-service getxxbyyy getgrbyname . . . 658
vserver services name-service getxxbyyy getgrlist . . . 658
vserver services name-service getxxbyyy gethostbyaddr . . . 659
vserver services name-service getxxbyyy gethostbyname . . . 660
vserver services name-service getxxbyyy getnameinfo . . . 661
vserver services name-service getxxbyyy getpwbyname . . . 662
vserver services name-service getxxbyyy getpwbyuid . . . 663
vserver services name-service getxxbyyy netgrpcheck . . . 664
vserver services name-service ldap check . . . 665
vserver services name-service ldap create . . . 666
vserver services name-service ldap delete . . . 667
vserver services name-service ldap modify . . . 668
vserver services name-service ldap show . . . 669
vserver services name-service ldap client create . . . 669
vserver services name-service ldap client delete . . . 674
vserver services name-service ldap client modify-bind-password . . . 675
vserver services name-service ldap client modify . . . 675
vserver services name-service ldap client show . . . 680
vserver services name-service ldap client schema copy . . . 683
vserver services name-service ldap client schema delete . . . 684
vserver services name-service ldap client schema modify . . . 684
vserver services name-service ldap client schema show . . . 687
vserver services name-service netgroup load . . . 690
vserver services name-service netgroup status . . . 691
vserver services name-service netgroup file delete . . . 693
vserver services name-service netgroup file show . . . 694
vserver services name-service nis-domain create . . . 695
vserver services name-service nis-domain delete . . . 696
vserver services name-service nis-domain modify . . . 696

vserver services name-service nis-domain show-bound . . . 697
vserver services name-service nis-domain show . . . 698
vserver services name-service nis-domain group-database build . . . 699
vserver services name-service nis-domain group-database status . . . 700
vserver services name-service nis-domain netgroup-database build . . . 701
vserver services name-service nis-domain netgroup-database show-status . . . 702
vserver services name-service nis-domain netgroup-database config modify . . . 703
vserver services name-service nis-domain netgroup-database config show . . . 704
vserver services name-service ns-switch create . . . 705
vserver services name-service ns-switch delete . . . 706
vserver services name-service ns-switch modify . . . 707
vserver services name-service ns-switch show . . . 709
vserver services name-service unix-group adduser . . . 710
vserver services name-service unix-group create . . . 711
vserver services name-service unix-group delete . . . 712
vserver services name-service unix-group deluser . . . 712
vserver services name-service unix-group load-from-uri . . . 713
vserver services name-service unix-group modify . . . 714
vserver services name-service unix-group show . . . 715
vserver services name-service unix-group file show . . . 716
vserver services name-service unix-group file status . . . 717
vserver services name-service unix-group max-limit modify . . . 719
vserver services name-service unix-group max-limit show . . . 719
vserver services name-service unix-user create . . . 720
vserver services name-service unix-user delete . . . 721
vserver services name-service unix-user load-from-uri . . . 721
vserver services name-service unix-user modify . . . 722
vserver services name-service unix-user show . . . 723
vserver services name-service unix-user file show . . . 724
vserver services name-service unix-user file status . . . 725
vserver services name-service unix-user max-limit modify . . . 727
vserver services name-service unix-user max-limit show . . . 727
vserver services name-service ypbind start . . . 728
vserver services name-service ypbind status . . . 728
vserver services name-service ypbind stop . . . 729
vserver services ndmp generate-password . . . 729
vserver services ndmp kill-all . . . 730
vserver services ndmp kill . . . 730
vserver services ndmp modify . . . 731
vserver services ndmp off . . . 737
vserver services ndmp on . . . 737
vserver services ndmp probe . . . 738
vserver services ndmp show . . . 743
vserver services ndmp status . . . 751
vserver services ndmp extensions modify . . . 756

vserver services ndmp extensions show . . . 757
vserver services ndmp log start . . . 757
vserver services ndmp log stop . . . 759
vserver services ndmp restartable-backup delete . . . 759
vserver services ndmp restartable-backup show . . . 760
vserver services web modify . . . 765
vserver services web show . . . 766
vserver services web access create . . . 769
vserver services web access delete . . . 769
vserver services web access show . . . 770
vserver smtape commands . . . 771
vserver smtape break . . . 771
vserver snapdiff-rpc-server commands . . . 772
vserver snapdiff-rpc-server off . . . 772
vserver snapdiff-rpc-server on . . . 772
vserver snapdiff-rpc-server show . . . 773
vserver vscan commands . . . 774
vserver vscan disable . . . 774
vserver vscan enable . . . 774
vserver vscan reset . . . 775
vserver vscan show-events . . . 775
vserver vscan show . . . 778
vserver vscan connection-status show-all . . . 779
vserver vscan connection-status show-connected . . . 781
vserver vscan connection-status show-not-connected . . . 783
vserver vscan connection-status show . . . 785
vserver vscan on-access-policy create . . . 787
vserver vscan on-access-policy delete . . . 789
vserver vscan on-access-policy disable . . . 790
vserver vscan on-access-policy enable . . . 791
vserver vscan on-access-policy modify . . . 792
vserver vscan on-access-policy show . . . 794
vserver vscan on-access-policy file-ext-to-exclude add . . . 797
vserver vscan on-access-policy file-ext-to-exclude remove . . . 798
vserver vscan on-access-policy file-ext-to-exclude show . . . 799
vserver vscan on-access-policy file-ext-to-include add . . . 800
vserver vscan on-access-policy file-ext-to-include remove . . . 801
vserver vscan on-access-policy file-ext-to-include show . . . 802
vserver vscan on-access-policy paths-to-exclude add . . . 803
vserver vscan on-access-policy paths-to-exclude remove . . . 804
vserver vscan on-access-policy paths-to-exclude show . . . 805
vserver vscan on-demand-task create . . . 806
vserver vscan on-demand-task delete . . . 809
vserver vscan on-demand-task modify . . . 810
vserver vscan on-demand-task run . . . 813

vserver vscan on-demand-task schedule . . . 814
vserver vscan on-demand-task show . . . 815
vserver vscan on-demand-task unschedule . . . 818
vserver vscan on-demand-task report delete . . . 819
vserver vscan on-demand-task report show . . . 820
vserver vscan scanner-pool apply-policy . . . 823
vserver vscan scanner-pool create . . . 824
vserver vscan scanner-pool delete . . . 826
vserver vscan scanner-pool modify . . . 827
vserver vscan scanner-pool resolve-hostnames . . . 829
vserver vscan scanner-pool show-active . . . 829
vserver vscan scanner-pool show . . . 832
vserver vscan scanner-pool privileged-users add . . . 835
vserver vscan scanner-pool privileged-users remove . . . 836
vserver vscan scanner-pool privileged-users show . . . 836
vserver vscan scanner-pool servers add . . . 837
vserver vscan scanner-pool servers remove . . . 838
vserver vscan scanner-pool servers show . . . 839

vserver commands

vserver add-aggregates

Add aggregates to the Vserver

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

Description

The `vserver add-aggregates` command adds aggregates to the Vserver.

Parameters

`-vserver <vserver>` - Vserver

Specifies the Vserver for which aggregates have to be added.

`-aggregates <aggregate name>,…` - List of Aggregates to Be Added

Specifies the list of aggregates to add to the Vserver. The root aggregates should not be specified in this list because though the command will return success, volumes cannot be created on root aggregates. In a MetroCluster configuration, this command does not honor the remote cluster's aggregates.

Examples

The following example illustrates how to add aggregates *`aggr1`* and *`aggr2`* to a Vserver named *`vs.example.com`*:

```
cluster1::> vserver add-aggregates -vserver vs.example.com -aggregates
aggr1,aggr2
```

vserver add-protocols

Add protocols to the Vserver

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

Description

The `vserver add-protocols` command adds given protocols to a specified Vserver.

Parameters

`-vserver <vserver>` - Vserver

This specifies the Vserver that is to be modified.

-protocols {nfs|cifs|fcp|iscsi|ndmp|nvme} - Protocols

This parameter specifies the list of protocols to be allowed to run on the Vserver. Possible values include *nfs* , *cifs* , *fcp* , *iscsi* , *ndmp* and *nvme* .

Examples

The following example shows adding protocol 'cifs' to a vserver named vs0.example.com.

```
cluster1::> vserver add-protocols -vserver vs0.example.com -protocols cifs
```

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::>
```

Related Links

- 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 to ensure unique Vserver names across cluster leagues.

Maximum number of characters supported is 47, and 41 for a Vserver with subtype "sync-source". "all" is a reserved name and must not be used as a Vserver name.

`[-subtype <vserver subtype>]` - Vserver Subtype

This specifies the subtype of the Vserver being created. Possible values are:

- default - For default data Vservers
- dp-destination - For Data Protection destination Vservers
- sync-source - For MetroCluster source Vservers
- sync-destination - For MetroCluster destination Vservers

`[-rootvolume <volume name>]` - Root Volume

This parameter optionally specifies the name of the Vserver's root volume, which is created when the Vserver is created. The default name is *`vserverName_root`* . The size of the Vserver's root volume is 1GB

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

This parameter optionally specifies the storage aggregate that holds the Vserver's root volume. Selection of the aggregate is based on the Vserver setup algorithm.

- Creating a root volume on the SnapLock aggregate is not supported.
- Creating a root volume of sync-source Vserver on the unmirrored aggregate is not supported.

`[-rootvolume-security-style <security style>]` - Root Volume Security Style

This parameter optionally 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). The default value is *`unix`* . Regardless of the security style, both NFS and CIFS clients can read from and write to the root volume.

`[-language <Language code>]` - Default Volume Language Code

This optionally specifies the default language encoding setting for the Vserver and its volumes. The recommended format is to append *`.UTF-8`* for the language encoding values. For example, for the *`en_US`* language, the recommended format is *`en_US.UTF-8`* . The default setting is *`C.UTF-8`* .

[-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.

[-data-services <LIF Service Name>,…] - Data Services

This optionally specifies the data services for new network interfaces created on the Vserver. If no value is specified, the default services list will be applied. This information will be used to construct the default service policies for this Vserver, which can be viewed using the `network interface service-policy show` command.

[-comment <text>] - Comment

This optionally specifies a comment for the Vserver.

[-quota-policy <text>] - Quota Policy

This optionally specifies a quota policy for the Vserver.

[-caching-policy <text>] - Caching Policy Name

This optionally specifies the caching policy to apply to the Vserver. A caching policy defines how the system caches this volume's data in Flash Cache modules. If a caching policy is not assigned to this Vserver, the system uses the default cluster-wide policy. The available caching policies are:

- none - Does not cache any user data or metadata blocks.
- auto - Read caches all metadata and randomly read user data blocks, and write caches all randomly overwritten user data blocks.

Default caching-policy is auto.

[-ipspace <IPspace>] - IPspace Name

This optionally specifies the IPspace the Vserver will be assigned to. If left unspecified, the Vserver will be assigned to the default IPspace.

[-foreground {true|false}] - Foreground Process

This parameter optionally specifies whether the Vserver create operation can be executed in the background. If nothing is specified, by default the Vserver create operation is executed in the foreground.

[-is-space-reporting-logical {true|false}] - Logical Space Reporting

This optionally specifies whether to report space logically on residing volumes. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

[-is-space-enforcement-logical {true|false}] - Logical Space Enforcement

This optionally specifies whether to perform logical space accounting on residing volumes. When space is enforced logically, ONTAP enforces volume settings such that all the physical space saved by the storage efficiency features will be calculated as used.

Examples

The following example creates a Vserver named *vs0.example.com* in the IPspace ipspace123. 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 language is U.S. English:

```
cluster1::> vserver create -vserver vs0.example.com -ipspace ipspace123
-rootvolume root_vs0 -aggregate aggr0
-language en_US.UTF-8 -rootvolume-security-style mixed
```

The following example creates a Vserver named *vs1* using default values. The default name for the Vserver's root volume is *vserverName_root* and the Vserver is located on an aggregate selected on the basis of the Vserver setup algorithm. The default root volume's security style is set to *unix* .

```
cluster1::> vserver create -vserver vs1
    cluster1::> vserver show -vserver vs1 -fields rootvolume, rootvolume-
security-style, aggregate
  vserver rootvolume aggregate rootvolume-security-style
  ------- ---------- --------- --------------------------
  vs1     vs1_root   aggr1     unix
```

Related Links

- volume create
- volume modify

vserver delete

Delete an existing 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 volumes, you must manually delete volumes (including root and mirror volumes) before you delete the Vserver. If the Vserver subtype is *dp-destination* , change the Vserver subtype to *default* by specifying the Vserver as the destination in the snapmirror break command before deleting the objects owned by the Vserver.

Parameters

-vserver <vserver> - Vserver

This specifies the Vserver that is to be deleted.

[-foreground {true|false}] - Foreground Process

This optionally specifies the Vserver delete operation can be executed in the background. If nothing is specified, by default the Vserver delete operation is executed in the foreground.

Examples

The following example deletes a Vserver named *vs2.example.com* :

```
cluster1::> vserver delete -vserver vs2.example.com
```

Related Links

- snapmirror break

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. If the Vserver subtype is of type *dp-destination* , then only the `-aggr-list` parameter can be modified.

Parameters

`-vserver <vserver>` - Vserver

This specifies the Vserver that is to be modified.

`[-language <Language code>]` - Default Volume Language Code

This optional parameter specifies the default language encoding setting for the Vserver and its volumes. The recommended format is to append *.UTF-8* for the language encoding values. For example, for the en_US language, the recommended format is *en_US.UTF-8* . The default setting is *C.UTF-8* .

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

This optional parameter specifies the Snapshot policy for a Vserver being modified.

`[-comment <text>]` - Comment

This optional parameter specifies a comment for the Vserver.

`[-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.

`[-aggr-list <aggregate name>,…]` - List of Aggregates Assigned

This optional parameter specifies a confined list of aggregates on which volumes can be created for a Vserver by the Vserver administrator. But these aggregates do not become exclusive property of the Vserver, i.e. they might be assigned for use to other Vservers. If the value of this parameter is specified as "-", then the Vserver administrator cannot create any volumes for that Vserver. Note that the cluster administrator will still be able to create volumes on any aggregate and assign them to this Vserver.

[-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.

[-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|fcp|iscsi|ndmp|nvme}] - Allowed Protocols

This optional parameter specifies the list of protocols to be allowed to run on the Vserver. When part of vserver-modify, this field should include the existing list along with the new protocol list to be added to prevent data disruptions. Possible values include *nfs* , *cifs* , *fcp* , *iscsi* , *ndmp* and *nvme* .

[-disallowed-protocols {nfs|cifs|fcp|iscsi|ndmp|nvme}] - Disallowed Protocols

This optional parameter specifies the list of protocols to be disallowed to run on the Vserver. When part of vserver-modify, this field should include the existing list along with the new protocol list to be added to prevent data disruptions. Possible values include *nfs* , *cifs* , *fcp* , *iscsi* , *ndmp* and *nvme* .

[-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".

[-caching-policy <text>] - Caching Policy Name

This optionally specifies the caching policy to apply to the Vserver. A caching policy defines how the system caches this volume's data in Flash Cache modules. If a caching policy is not assigned to this Vserver, the system uses the default cluster-wide policy. The available caching policies are:

- none - Does not cache any user data or metadata blocks.
- auto - Read caches all metadata and randomly read user data blocks, and write caches all randomly overwritten user data blocks.

Default caching-policy is auto.

[-is-space-reporting-logical {true|false}] - Logical Space Reporting

This optionally specifies whether to report space logically on residing volumes which are created after this operation. Existing volumes will not be affected by modifying this value on an existing Vserver. To change whether space is reported logically for existing volumes, you will have to modify the setting on those volumes. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

[-is-space-enforcement-logical {true|false}] - Logical Space Enforcement

This optionally specifies whether to perform logical space accounting on residing volumes which are created after this operation. Older volumes will continue to have old value. When space is enforced logically, ONTAP enforces volume settings such that all the physical space saved by the storage efficiency features will be calculated as used.

Examples

The following example modifies the quota policy for a Vserver named vs0.example.com to pol1, specifies a Snapshot policy named daily, adds the comment "Sales team access".

```
cluster1::> vserver modify -vserver vs0.example.com -snapshot-policy daily
    -comment "Sales team access" -quota-policy pol1
```

vserver prepare-for-revert

Prepares Vservers to be reverted

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

Description

The `vserver prepare-for-revert` command prepares Vservers to be reverted to the previous version of Data ONTAP. It disables any operations that cannot be scheduled during revert.

Examples

The following example prepares all Vservers to be reverted.

```
cluster1::*> vserver prepare-for-revert
```

vserver remove-aggregates

Remove aggregates from the Vserver

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

Description

The `vserver remove-aggregates` command removes aggregates from the Vserver.

Parameters

`-vserver <vserver>` - Vserver

Specifies the Vserver from which aggregates have to be removed.

`-aggregates <aggregate name>,…` - List of Aggregates to Be Removed

Specifies the list of aggregates to remove from the Vserver.

Examples

The following example illustrates how to remove aggregates *`aggr1`* and *`aggr2`* from a Vserver named *`vs.example.com`*:

```
cluster1::> vserver remove-aggregates -vserver vs.example.com -aggregates
aggr1,aggr2
```

vserver remove-protocols

Remove protocols from the Vserver

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

Description

The `vserver remove-protocols` command removes the specified protocols from the specified Vserver. When you remove the protocols from a Vserver, the data access with respect to the removed protocols is disrupted.

Parameters

`-vserver <vserver>` - Vserver

Specifies the Vserver that is to be modified.

`-protocols {nfs|cifs|fcp|iscsi|ndmp|nvme}` - Protocols

This parameter specifies the list of protocols to be removed. on the Vserver. Possible values include *`nfs`* , *`cifs`* , *`fcp`* , *`iscsi`* , *`ndmp`* and *`nvme`* .

Examples

The following example shows removing protocol 'cifs' from a Vserver named vs0.example.com.

```
cluster1::> vserver remove-protocols -vserver vs0.example.com -protocols
cifs
```

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. If the vserver being renamed is participating in an Inter-cluster Vserver peer relationship, all the corresponding remote clusters will be updated with the new peer Vserver name.

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.

Maximum number of characters supported is 47, and 41 for a Vserver with subtype "sync-source". "all" is a reserved name and must not be used as a Vserver name.

[-foreground {true|false}] - Foreground Process

This specifies whether the rename job will be run in foreground or backgound. By default, the job runs in foreground.

Examples

The following examples rename a Vserver named *vs1.example.com* as *vs2.example.com* , and then finally back to its original name:

```
(When there is no intercluster Vserver peer relationship with the vserver)
cluster1::> vserver rename -vserver vs1.example.com -newname
vs2.example.com
(When there is at least one intercluster peer relationship with the
Vserver)
cluster1::> vserver rename -vserver vs1.example.com -newname
vs2.example.com
[Job 277] Job succeeded: Vserver rename completed successfully
cluster1::> vserver rename -vserver vs2.example.com -newname
vs1.example.com -foreground false
[Job 278] Job is queued: Rename Vserver vs2.example.com to
vs1.example.com.
```

vserver restamp-msid

Restamp the MSIDs of all the volumes in a Vserver to match or be different from the source Vserver

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

Description

The `vserver restamp-msid` command restamps MSIDs of all volumes in a dp-destination Vserver to make them either identical to the VserverDR source Vserver. The command is run on secondary VserverDR site and automatically updates the MSID preserve behavior for the Vserver. A snapmirror resync must be run after this command completes.

Parameters

`-vserver <vserver name>` - Vserver name (privilege: advanced)

The name of the dp-destination Vserver.

`-preserve-msid {true|false}` - Make MSID same as that of source Vserver. False sets the values as different. (privilege: advanced)

Boolean value through which the user can specify whether to make the MSIDs of the volumes same as that of Source Vserver. Specifying true will make the MSIDs same and specifying false will make them different.

Examples

This example will stamp all the volumes of Vserver vs1dp with the same MSID as the source Vserver.

```
cluster1::>vserver restamp-msid -vserver vs1dp -preserve-msid true
```

Related Links

- snapmirror resync

vserver show-aggregates

Show details of aggregates in a Vserver

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

Description

The `vserver show-aggregates` command displays the details of all the aggregates that are associated with Vservers. The aggregate details displayed are the aggregate name, state, available size, the type of aggregate and the SnapLock type.

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

If this optional parameter is specified, the command displays the details of aggregates that are associated with the specified Vserver.

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

If this optional parameter is specified, the command displays all of the Vservers configured with the specified aggregate.

Examples

The following example displays the aggregates configured for Vserver vs.

```
cluster1::> vserver show-aggregates -vserver vs
                                       Available
Vserver        Aggregate      State          Size Type    SnapLock-Type
-------------- -------------- ------- ---------- ------- -------------
vs             aggr1          online     795.2MB hdd     non-snaplock
vs             aggr2          online     795.2MB hdd     non-snaplock
2 entries were displayed.
```

vserver show-protocols

Show protocols for Vserver

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

Description

The `vserver show-protocols` command displays the running protocols on a given 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>] - Vserver

If this parameter is specified, the command displays the allowed set of protocols for the specified Vserver.

[-protocol {nfs|cifs|fcp|iscsi|ndmp|nvme}] - Protocols

If this optional parameter is specified, the command displays all the Vservers configured with the specified protocols.

Examples

The following example displays the protocols configured for Vserver vs1.

```
cluster1::> vserver show-protocols -vserver vs1
  Vserver: vs1
  Protocols: nfs, cifs
```

vserver show

Display Vservers

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

Description

The `vserver show` command displays the following information:

- Vserver name
- Vserver type (*`data`* , *`admin`* , *`node`* or *`system`* - detailed view only)
- Vserver subtype (*`default`* , *`dp-destination`* , *`sync-source`* , and *`sync-destination`* - detailed view only)
- Vserver universal unique identifier (detailed view only)
- Root volume name
- Aggregate on which the root volume is located
- Associated NIS domain
- Root volume security style (*`unix`* for UNIX mode bits, *`ntfs`* for CIFS ACLs, *`mixed`* for both (detailed view only)
- LDAP client
- Language (detailed view only)
- Snapshot policy (detailed view only)
- Comment text (detailed view only)
- Quota policy (detailed view only)
- Aggregate list (detailed view only)
- Maximum Volumes (detailed view only)
- Qos-policy-group (detailed view only)
- Config-lock (detailed view only)
- Admin state (*`running`* , *`stopped`* , *`starting`* , *`stopping`* , *`initializing`* , or *`deleting`*)
- Operational state (*`running`* , or *`stopped`*)
- Operational state stopped reason (*`sync-destination-and-switchover-not-done`* , or *`cluster-reboot-done`* , or *`admin-state-stopped`*)
- Allowed Protocols (*`nfs`* , *`cifs`* , *`fcp`* , *`iscsi`* , *`nvme`* , *`ndmp`* - detailed view only)
- Disallowed Protocols (*`nfs`* , *`cifs`* , *`fcp`* , *`iscsi`* , *`nvme`* , *`ndmp`* - detailed view only)
- IPspace to which the Vserver belongs (detailed view only)
- Caching policy

Parameters

{ [-fields <fieldname>,…]

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

| [-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, *system* for cluster-level communications in an IPspace, *data* for data serving Vserver, and *node* for node management Vserver.

[-subtype <vserver subtype>] - Vserver Subtype

If this parameter is specified, the command displays information only about the Vserver or Vservers that have the specified Vserver subtype. Types include:

- *default* for default data Vserver
  *
  and
- *dp-destination* for Data Protection destination Vserver.
- *sync-source* for MetroCluster source Vserver,
- *sync-destination* for MetroCluster destination Vserver.

[-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.

[-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 <security style>] - 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.

[-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 and at the Vserver 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.

[-data-services <LIF Service Name>,…] - Data Services

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified data services.

[-comment <text>] - Comment

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified comment.

[-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

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified admin-state.

[-operational-state {running|stopped}] - Vserver Operational State

If this parameter is specified, the command displays information only about the Vserver or Vservers that match the specified operational-state. This field determines the state of the Vserver LIFs. New LIFs created on a Vserver, which is in running state, will be operationally up and the LIFs created on a Vserver, which is in stopped state, will be operationally down.

[-operational-state-stopped-reason {sync destination and switchover is not done|cluster reboot is done|admin state stopped| dp destination not started}] - Vserver Operational State Stopped Reason

If this parameter is specified, the command displays information only about the Vserver or Vservers that are operationally stopped due to the specified reason. This field indicates the reason for the operational-state of the Vserver being stopped

[-allowed-protocols {nfs|cifs|fcp|iscsi|ndmp|nvme}] - 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|fcp|iscsi|ndmp|nvme}] - 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 no longer supported.

[-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.

[-caching-policy <text>] - Caching Policy Name

Display the Vservers that match the specified caching-policy.

A caching policy defines the caching behavior of this Vserver at the Flash Cache level. If a caching policy is not assigned to this Vserver, the system uses the default cluster-wide policy. The available caching policies are:

- none - Does not cache any user data or metadata blocks.
- auto - Read caches all metadata and randomly read user data blocks, and write caches all randomly overwritten user data blocks.

Default caching-policy is auto.

[-config-lock {true|false}] - Config Lock

This parameter specifies if the Vserver is locked or unlocked for modification. If the config-lock is set to true, then modifying the Vserver’s configuration is not allowed.

[-ipspace <IPspace>] - IPspace Name

If this parameter is specified, the command displays information only about the Vservers that are assigned to the specified IPspace.

[-foreground {true|false}] - Foreground Process

This optionally specifies whether the Vserver show operation can be executed in the background. If nothing is specified, by default the Vserver show operation is executed in the foreground.

[-is-space-reporting-logical {true|false}] - Logical Space Reporting

This optionally specifies whether to report space logically on residing volumes. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also as reported as used.

[-is-space-enforcement-logical {true|false}] - Logical Space Enforcement

This optionally specifies whether to perform logical space accounting on residing volumes. When space is enforced logically, ONTAP enforces volume settings such that all the physical space saved by the storage efficiency features will be calculated as used.

Examples

The following example displays information about all Vservers.

```
cluster1::> vserver show

non mcc setup:
                  Admin    Operational   Root
Vserver      Type    Subtype        state    state      Volume  Aggregate
-----------   ------- --------------- ----------- ----------- -----------
---------
cluster      admin   -          -    -           -    -
node1      node    -          -    -           -    -
vs0        data    default        running  running      root_vs1  aggr0
vs1        data    dp-destination   stopped  stopped      -    -

4 entries were displayed.

mcc setup:

cluster1::> vserver show
                  Admin   Operational Root
Vserver      Type    Subtype         state   state       Volume
Aggregate
----------    ------- ---------------   ------- ----------- -----------
---------
cluster      admin   -        -    -       -      -
node1      node    -        -    -       -      -
vs2           data    sync-source    running  running   rv
data_aggr
vs3-mc      data    sync-destination  running  stopped  -      -

4 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 the data access is to be started. This operation is only supported on a data Vserver.

The name must be of 47 characters length 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.

`[-force <true>]` - Force Vserver Start

In case of a MetroCluster configuration or Vserver disaster recovery, by using this parameter you can start the Vserver that is either locked (which prevents any configuration changes) or its partner Vserver is operationally running. If you do not enter this parameter, it is set to false.

Examples

The following example starts data access on Vserver *`vs0.example.com`* in the background.

```
cluster1::> 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 the data access is to be stopped. This operation is only supported on a data Vserver.

The name must be of 47 characters length 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.

```
cluster1::> vserver stop -vserver vs0.example.com -foreground false
```

vserver unlock

Unlock Vserver configuration

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

Description

The `vserver unlock` command revokes the administrative lock on the Vserver configuration. When a Vserver is unlocked, changes to the configuration are permitted. The unlock operation fails if the Vserver is not locked by the administrator or if it is locked by internal applications. If the Vserver fails to unlock due to an error condition, you can use the -force option.

Parameters

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

The name of the Vserver that has to be unlocked.

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

This option is specified to unlock the Vserver when the Vserver fails to unlock due to an error condition.

Examples

The following example illustrates how to unlock the Vserver named *vs123.example.com, forcefully*:

```
cluster1::> vserver unlock -vserver vs1.example.com -force true
```

vserver active-directory commands

vserver active-directory create

Create an Active Directory account. If joining a domain, this command may take several minutes to complete.

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

Description

The `vserver active-directory create` command creates an Active Directory account for a Vserver. When you create the Active Directory account, you must add it to an existing Windows Active Directory domain. When you enter this command, you are prompted 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. When joining a domain, this command may take several minutes to complete.

Each Vserver can have only one Active Directory account.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the name of the Vserver for which you want to create the Active Directory account. The Vserver must already exist.

`-account-name <NetBIOS>` - Active Directory NetBIOS Name

This parameter specifies the name of the Active Directory account (up to 15 characters).

`-domain <TextNoCase>` - Fully Qualified Domain Name

This parameter specifies the name of the Active Directory domain.

`[-ou <text>]` - Organizational Unit

This parameter specifies the organizational unit within the Active Directory domain. By default, this parameter is set to *`CN=Computers`* . When specifying this parameter, specify only the organizational unit portion of the distinguished name. Data ONTAP appends the value provided for the required `-domain` parameter onto the value provided for `-ou` parameter to produce the Active Directory distinguished name, which is used when creating the Vserver's Active Directory account in the domain.

Nested OUs must be provided in a specific order with all containers separated by a comma. Reading from left to right you travel up the directory tree until you reach the root OU.

Examples

The following example creates an Active Directory account *`ADSERVER1`* for Vserver *`vs1`* and domain *`example.com`* .

```
cluster1::> vserver active-directory create -vserver vs1 -account-name
ADSERVER1 -domain example.com

In order to create an Active Directory machine account, 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:
```

The following example creates an Active Directory account *ADSERVER2* for Vserver *vs2* , domain *example.com* and organizational unit *sample_ou* .

```
cluster1::> vserver active-directory create -vserver vs2 -account-name
ADSERVER2 -domain example.com -ou OU=sample_ou

In order to create an Active Directory machine account, you must supply
the
name and password of a Windows account with sufficient privileges to add
computers to the "OU=sample_ou" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:
```

The following example creates an Active Directory account *ADSERVER2* for Vserver *vs2* , domain *example.com* and nested organizational unit *OU=developers,OU=engineering,OU=corp* .

```
cluster1::> vserver active-directory create -vserver vs2 -account-name
ADSERVER2 -domain example.com -ou OU=developers,OU=engineering,OU=corp

In order to create an Active Directory machine account, you must supply
the
name and password of a Windows account with sufficient privileges to add
computers to the "OU=developers,OU=engineering,OU=corp" container within
the "example.com" domain.

Enter the user name: Administrator

Enter the password:
```

vserver active-directory delete

Delete an Active Directory account

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

Description

The `vserver active-directory delete` command deletes the Active Directory account for a specified Vserver.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the Vserver for the Active Directory account you want to delete.

Examples

The following example deletes the Active Directory account for a Vserver named *vs1* :

```
cluster1::> vserver active-directory delete -vserver vs1
In order to delete an Active Directory machine account, you must supply
the
name and password of a Windows account with sufficient privileges to
remove
computers from the "example.com" domain.

Enter the user name: Administrator

Enter the password:
```

vserver active-directory modify

Modify the domain of an Active Directory account. If re-joining the current domain or joining a new one, this command may take several minutes to complete.

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

Description

The `vserver active-directory modify` command modifies the domain of an Active Directory account. You can also re-join the current domain or join a new one. When joining a domain, this command may take several minutes to complete.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the Vserver for the Active Directory account whose associated domain 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 Active Directory account.

Examples

The following example modifies the Active Directory domain associated with Vserver *vs1* .

```
cluster1::> vserver active-directory modify -vserver vs1 -domain
example.com

In order to create an Active Directory machine account, 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 active-directory password-change

Change the domain account password for an Active Directory account

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

Description

The `vserver active-directory password-change` command changes the domain account password for the specified Vserver's Active Directory account.

Parameters

-vserver <vserver> - Vserver

This parameter specifies the name of the Vserver associated with the Active Directory account whose domain account password you want to change.

Examples

The following example changes the password for the Active Directory account for a Vserver named *vs1* .

```
cluster1::> vserver active-directory password-change -vserver vs1
```

vserver active-directory password-reset

Reset the domain account password for an Active Directory account

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

Description

The `vserver active-directory password-reset` command resets the domain account password for the Active Directory account. 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 contains the machine account.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the name of the Vserver associated with the Active Directory account whose domain account password you want to reset.

Examples

The following example resets the password for the Active Directory account for a Vserver named *`vs1`* .

```
cluster1::> vserver active-directory password-reset -vserver vs1

Enter your user ID: Administrator
Enter your password:
```

vserver active-directory show

Display Active Directory accounts

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

Description

The `vserver active-directory show` command displays information about Active Directory accounts. 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 Active Directory accounts:

- Vserver name
- Active Directory account NetBIOS name
- Domain or workgroup name

You can specify the `-fields` parameter to specify which fields of information to display about Active Directory accounts. You can use `-fields ?` to display the valid values for the `-fields` parameter. In addition to the fields above, you can display the following fields:

- Fully-qualified domain name
- Organizational unit

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about Active Directory accounts that are in the Windows Active Directory domain

named *RUBY* , run the command with the value of the `-domain-workgroup` parameter set to *RUBY* .

You can specify the `-instance` parameter to display all information for all Active Directory accounts 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.

[-vserver <vserver>] - Vserver

If you specify this parameter, the command displays information only about the Active Directory account for the specified Vserver.

[-account-name <NetBIOS>] - Active Directory NetBIOS Name

If you specify this parameter, the command displays information only for the Active Directory accounts that match the specified NetBIOS account name.

[-domain-workgroup <CIFS domain>] - NetBIOS Domain/Workgroup Name

If you specify this parameter, the command displays information only for the Active Directory accounts that are in the specified NetBIOS domain or workgroup.

Workgroups are not supported in this release.

[-domain <TextNoCase>] - Fully Qualified Domain Name

If you specify this parameter, the command displays information only for the Active Directory accounts that are in the specified domain.

[-ou <text>] - Organizational Unit

If you specify this parameter, the command displays information only for the Active Directory accounts that are in the specified organizational unit.

[-auth-style {domain|workgroup|realm}] - Authentication Style

If you specify this parameter, the command displays information only for the Active Directory accounts that are in the specified authentication style.

Examples

The following example displays a subset of the information about all Active Directory accounts.

```
cluster1::> vserver active-directory show
Account     Domain/Workgroup
 Vserver        Name        Name
 -------------- ----------- ---------------
 vs1            ADSERVER1   EXAMPLE
```

The following example displays all information about all Active Directory Vservers in list form.

```
cluster1::> vserver active-directory show -instance
Vserver: vs1
            Active Directory account NetBIOS Name: ADSERVER1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
```

vserver audit commands

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.

Parameters

`-vserver <vserver name>` - Vserver

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

`-destination <text>` - Log Destination Path

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

`[-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|authorization-policy-change|security-group}]` - Categories of Events to Audit

This parameter specifies the categories of events to be audited. Supported event categories are: file access events (both CIFS and NFS), CIFS logon and logoff events, Central Access Policy(CAP) staging events, File share events, Audit policy change events, Local User Account Management Events, Local Security Group Management Events and Authorization Policy Change Events. The corresponding parameter values are: *`file-ops`* , *`cifs-logon-logoff`* , *`cap-staging`* , *`file-share`* , *`audit-policy-change`* , *`user-account`* , *`security-group`* and *`authorization-policy-change`* .By default, *`file-ops`* , *`cifs-logon-logoff`* and *`audit-policy-change`* events are enabled. The support for *`audit-policy-change`* event can be modified from diag promt using vserver audit modify command.

`[-format {xml|evtx}]` - Log Format

This parameter specifies the output format of the audit logs. The output format can be either Data ONTAP-specific XML or Microsoft Windows EVTX log format. By default, the output format is EVTX.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
cluster1::> 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
```

The following example creates an audit configuration for Vserver vs1 for auditing CIFS and NFS file access events in the output log format EVTX.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-format evtx -events file-ops
```

Related Links

- vserver audit modify

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 ignore errors while enabling auditing.

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, the command fails. The path can be up to 864 characters in length and must have read-write permissions.

[-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|authorization-policy-change|security-group}] - Categories of Events to Audit

This parameter specifies the categories of events to be audited. Supported event categories are: file access events (both CIFS and NFS), CIFS logon and logoff events, Central Access Policy(CAP) staging events, File share events, Audit policy change events, Local User Account Management Events, Local Security Group Management Events and Authorization Policy Change Events. The corresponding parameter values are: *file-ops* , *cifs-logon-logoff* , *cap-staging* , *file-share* , *audit-policy-change* , *user-account* , *security-group* and *authorization-policy-change* . By default, *file-ops* , *cifs-logon-logoff* and *audit-policy-change* events are enabled

[-format {xml|evtx}] - Log Format

This parameter specifies the output format of the audit logs. The output format can be either Data ONTAP-specific XML or Microsoft Windows EVTX log format. By default, the output format is EVTX.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
cluster1::> vserver 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
```

The following example modifies an audit configuration for Vserver vs1 for auditing CIFS and NFS file access events in the output log format EVTX.

```
cluster1::> vserver audit modify -vserver vs1 -format evtx -events file-
ops
```

vserver audit prepare-to-downgrade

Restore the Audit configuration to Earlier Release of Data ONTAP

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

Description

The `vserver audit prepare-to-downgrade` command restores the Audit configurations for ONTAP based on the input parameter disable-feature-set.

Parameters

`-disable-feature-set <downgrade version>` - Data ONTAP Version (privilege: advanced)

This parameter specifies the ONTAP version that introduced the new Audit features and needs to be removed. The value can be one of the following:

- 9.0.0 - Disables the Audit features introduced in the ONTAP release 9.0.0. The following events are removed from the `event` list:
- File share event. The corresponding parameter value is *`file-share`* .
- Audit policy change event. The corresponding parameter value is *`audit-policy-change`* .
- Local user account management event. The corresponding parameter value is *`user-account`* .
- Local security group management event. The corresponding parameter value is *`security-group`* .
- Authorization policy change event. The corresponding parameter value is *`authorization-policy-change`* .

Examples

```
cluster1::*> vserver audit prepare-to-downgrade -disable-feature-set 9.0.0
```

vserver audit rotate-log

Rotate audit log

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

Description

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

Parameters

`-vserver <vserver name>` - Vserver

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

Examples

The following example rotates audit logs for Vserver vs1.

```
cluster1::> vserver audit rotate-log -vserver vs1
```

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.

[-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|authorization-policy-change|security-group}] - Categories of Events to Audit

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

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

[-format {xml|evtx}] - Log Format

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
cluster1::> vserver audit show
Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /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
Rotation                            Rotation
 Vserver     File Size Rotation Schedule        Limit
 ----------- --------- ------------------------ --------
 vs1         100MB     -                        0
```

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

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

vserver audit audit-log-redirect create

Create Audit Log Redirect Vserver destination

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

Description

The `vserver audit audit-log-redirect create` command creates an audit log redirect configuration to designate a dedicated Vserver for all audit logs in a cluster to reside in.

Parameters

`-vserver <vserver name>` - Audit Log Redirect Vserver (privilege: advanced)

Use this parameter to specify a dedicated Vserver for all audit logs to reside in.

Examples

The following example causes all audit logs in a cluster to be redirected to *`vserver1`* :

```
cluster1::> vserver audit audit-log-redirect create -vserver vserver1
```

vserver audit audit-log-redirect delete

Delete Audit Log Redirect Vserver destination

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

Description

The `vserver audit audit-log-redirect delete` command deletes the dedicated Vserver for all audit logs in a cluster to reside in.

Examples

The following example delete the audit-log-redirect Vserver.

```
cluster1::> vserver audit audit-log-redirect delete
```

vserver audit audit-log-redirect modify

Modify Audit Log Redirect Vserver destination

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

Description

The `vserver audit audit-log-redirect modify` command changes the dedicated Vserver for all audit logs in a cluster to reside in.

Parameters

`[-vserver <vserver name>]` - Audit Log Redirect Vserver (privilege: advanced)

Use this parameter to specify a dedicated Vserver for all audit logs to reside in.

Examples

The following example modify the current audit-log-redirect Vserver to *`vserver1`* :

```
cluster1::> vserver audit audit-log-redirect modify -vserver vserver1
```

vserver audit audit-log-redirect show

Display Audit Log Redirect Vserver destination

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

Description

The `vserver audit audit-log-redirect show` command displays the dedicated Vserver for all audit logs in a cluster to reside in.

Examples

The following example displays the audit-log-redirect Vserver:

```
cluster1::> vserver audit audit-log-redirect show
Audit Log Redirect Vserver: vserver1
```

vserver check commands

vserver check lif-multitenancy run

Run check for LIF multitenancy

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

Description

The run command checks the specified Vserver to verify that it has connectivity to the configured external servers providing services such as Active Directory, NIS, and DNS. The output can consist of three types of messages. Failure messages indicate that a Vserver does not have the connectivity required to a server exporting a service. Warning messages indicate configuration or operational issues that are possible causes of the failures. A success message is displayed if the Vserver has network connectivity to each of the configured servers for each service.

You can use this command to verify configuration changes such as creating a Vserver or changing the configured servers for one or more services. It is also useful for diagnosing operational problems that result from failures that could be caused by the inability to make network connections to configured servers.

The services that are checked are DNS, NIS, CIFS preferred domain controllers, CIFS discovered domain controllers, KDC, Active Directory, Admin, Password, LDAP, and LDAP preferred Active Directory.

Only a single run for a Vserver is allowed to run in a cluster. If multiple runs are attempted for a Vserver, a message will be displayed indicating that a run is already in progress.

For each service, this command will ping each configured server until a successful ping is completed. In certain circumstances where a subnet is offline or LIFs are operationally down, this command may take a long time to

run. In order to show that forward progress is being made, an activity indicator of a '.' is displayed for each ping sent.

The following fields are reported in table format. Some fields may not be relevant to a type of message and will consist of the text "-".

- Vserver name
- Service external server is exporting
- Address of external server
- Connectivity to that external server
- More information describing the problem
- Suggestions to remediate the problems
- Success when there are no problems

Parameters

`-vserver <vserver>` - Vserver

Use this parameter to specify the Vserver to check.

`[-verbose {true|false}]` - Show Positive and Negative Result (privilege: advanced)

When this parameter is specified the results of all connectivity tests will be displayed in the success and failure cases.

Examples

```
This is an example of a successful run:
```

```
cluster1::> vserver check lif-multitenancy run -vserver vs0
     ..
     SUCCESS: All external servers are reachable.
```

This is an example of a run with warnings and failures that need to be corrected:

```
cluster1::> vserver check lif-multitenancy run -vserver vs0
     Vserver         Severity Service            Address         LIF
Connected  Details
     -------------- -------- ------------------ --------------
-------------- ---------- --------------
     vs0             warning  -                  -               vs0_lif1
-          operationally down
     vs0             warning  -                  -               vs0_lif2
-          operationally down
     ...
     vs0             failure  DNS                10.98.200.20    -
no         cache
     ...
     vs0             failure  NIS domain         10.98.13.53     -
no         cache
Error : command failed:   FAILURES FOUND.
             You must correct these failures to avoid service disruptions
             in DOT 8.3 and above.
             Corrective actions may include:
               - removing decommissioned external servers from the vserver
            configuration
               - restoring network interfaces that are down
               - adding network interfaces or routes
               - modifying the locations where network interfaces may
reside
            (through
                 adjusting failover groups/policies or changing the home-
node or
                 auto-revert settings).
             For assistance, please consult the 8.3 Upgrade Document,
             or contact support personnel.
```

vserver check lif-multitenancy show-results

Show the results of the latest multitenancy network run

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

Description

You can view detailed information about the latest completed run, or the run for a Vserver.

- Vserver - name of vserver run was for
- Severity - severity of the message which is failure, warning, or info.
  *
  Failures are problems that need fixed. Warnings are potential

problems that may need to be fixed. Values are "failure", "warning" or "info".

- Service - name of service that is being checked for connectivity
- Address - address of server configured for the above service that is being
  *
  checked for connectivity.
- LIF - the LIF a successful connectivity check to the above server was made from
- Connected - true of there is connectivity, false if there is not
- Status - additional information useful for resolving issues

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

Selects the messages matching the specified Vserver

[-severity <text>] - Severity

Selects the messages matching the specified severity of failure, warning, and info.

[-service <text>] - Service Name

Selects the messages matching the specified service.

[-address <text>] - Address of Server

Selects the messages matching the specified address.

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

Selects the messages matching the specified LIF.

[-connected {yes|no}] - Vserver Connectivity

Selects the messages matching the specified connectivity.

[-status <text>] - Additional Information

Selects the messages matching the specified search criteria.

Examples

Runs that are successful will not have any content.

```
cluster1::> vserver check lif-multitenancy show-results -vserver vs0
     This table is currently empty.
```

Runs that fail display each failure that needs to be fixed.

```
cluster1::> vserver check lif-multitenancy show-results -vserver vs0
                                        Network      Logical
     Vserver     Severity  Service      Address      Interface  Connected
Status
     ----------  --------  -----------  -----------  ---------  ----------
-------
     vs0
                 warning   -            -            vs0_lif1   -
operationally down
                 warning   -            -            vs0_lif2   -
operationally down
                 failure   DNS          10.98.200.20
                                                     -          no
cache
                 failure   NIS domain   10.98.13.53  -          no
cache
     4 entries were displayed.
```

vserver check lif-multitenancy show

Show the summary of the latest multitenancy network run

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

Description

You can view summary information about the latest completed run, or the run in progress for a Vserver. It will show the following fields:

- Vserver - Name of Vserver that was checked for LIF connectivity
- Start Time - Date And Time the run was started
- Status - Not Started, In Progress, Complete, or Aborted
- Success - Yes if the run has a Status of Complete with no failures. No if the run has a status of Complete with one or more failures.

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

Selects the summary information matching the specified Vserver.

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

Selects the summary information matching the specified date and time the run was started

[-status {not started|in progress|complete|aborted}] - Run Status

Selects the summary information matching the specified status of the run.

[-success {yes|no}] - Successful Run

Selects the summary information matching the specified success or failure of the run.

[-updated <MM/DD/YYYY HH:MM:SS>] - Run Updated

Selects the summary information matching the last time the run was still in progress.

Examples

This is what a successful run looks like:

```
cluster1::> vserver check  lif-multitenancy show
     Vserver         Start Time           Status        Success
     --------------  -------------------  ------------  -------
     vs0
                     7/16/2014 14:28:35   complete      yes
```

This is what a failed run looks like:

```
cluster1::> vserver check lif-multitenancy show
     Vserver         Start Time           Status        Success
     --------------  -------------------  ------------  -------
     vs0
                     7/16/2014 14:40:55   complete      no
```

This is what specifying the Vserver looks like:

```
cluster1::> vserver check lif-multitenancy show -vserver vs0
Vserver: vs0
        Start Time: 7/16/2014 14:40:55
        Run Status: complete
     Successful Run: no
```

vserver cifs commands

vserver cifs add-netbios-aliases

Add NetBIOS aliases for the CIFS server name

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

Description

```
The `vserver cifs add-netbios-aliases` command creates or adds a list of
NetBIOS aliases for the CIFS server name.
```

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for which NetBIOS alias are to be created or added.

`-netbios-aliases <NetBIOS>,…` - List of NetBIOS Aliases

This parameter specifies one or more NetBIOS aliases to be added to an existing list of NetBIOS aliases. A new list of NetBIOS aliases is created if the list is currently empty.

Examples

The following example creates a new list of NetBIOS aliases for Vserver vs_a.

```
cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: -

cluster1::> cifs add-netbios-aliases -netbios-aliases
alias_1,alias_2,alias_3

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example adds several NetBIOS aliases for the CIFS server CIFS_SERVER on Vserver vs_a.

```
cluster1::> cifs add-netbios-aliases -netbios-aliases
alias_4,alias_5,alias_6

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a

      Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                   ALIAS_5, ALIAS_6

cluster1::> vserver cifs add-netbios-aliases -vserver v1 -netbios-aliases
alias_7

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a

      Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                   ALIAS_5, ALIAS_6, ALIAS_7
```

vserver cifs check

Display Validation Status of CIFS Configuration from Each Node

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

Description

Use the `vserver cifs check` command to check the status of configured CIFS server on a particular 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 specify the Vserver whose CIFS server needs to be validated.

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

Use this parameter to specify the node name from which CIFS server connectivity needs to be validated.

[-netbios-name <TextNoCase>] - CIFS NetBIOS Name

Use this parameter to display netbios-name of the configured CIFS server.

[-cifs-status <TextNoCase>] - CIFS Server Status

Use this parameter to display status of configured CIFS server.

[-site <TextNoCase>] - CIFS Server Site

This parameter specifies the site discovered from Data ONTAP for the Active Directory domain associated with the CIFS server. If the discovery fails, this parameter will be updated with the default-site of associated cifs server.

[-server <TextNoCase>] - Domain Controller Name

Use this parameter to display Domain name of the configured CIFS server.

[-server-ip <text>] - Domain Controller IP Addr

Use this parameter to display IP-address of the configured CIFS server.

[-status {down|up}] - Connectivity Status

Use this parameter to display information only about CIFS servers with a status that matches the value you specify.

[-status-details <text>] - Connectivity Status Details

Use this parameter to display information only about CIFS servers with status details that match the value you specify.

Examples

The following example checks the connectivity of CIFS server on vserver vs0 from each node.

```
cluster1::> vserver cifs check -vserver vs0
Vserver : vs0
                Cifs NetBIOS Name : NEWSERVER
                      Cifs Status : up
                             Site : Bangalore

Node Name DC Server Name    DC Server IP  Status  Status Details
--------- ----------------  ------------  ------- --------------
node1     CIFSSERVER.COM    10.11.12.13    up     Response time (msec): 55
node2     CIFSSERVER.COM    10.11.12.13    up     Response time (msec): 70
node3     CIFSSERVER.COM    10.11.12.13    down   Secd: No Server
available.
```

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 can add it to an existing CIFS domain, or you can join it to a workgroup. When you add it to an existing CIFS domain, 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. If the new CIFS server is joining a domain, this command might take several minutes to complete.

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. When specifying this parameter, specify only the organizational unit portion of the distinguished name. Data ONTAP appends the value provided for the required `-domain` parameter onto the value provided for `-ou` parameter to produce the Active Directory distinguished name, which is used to associate with the CIFS server.

Nested OUs must be provided in a specific order with all containers separated by a comma. Reading from left to right you travel up the directory tree until you reach the root OU.

`[-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.

`| -workgroup <NetBIOS>` - Workgroup Name `}`

This parameter specifies the name of the workgroup (up to 15 characters).

`[-keytab-uri {(ftp|http)://(hostname|IPv4 Address|'['IPv6 Address']')…}]` - Kerberos Keytab File URI (privilege: advanced)

This parameter specifies loading a keytab file from the specified URI. This is applicabe if the CIFS server is being created in realm mode or domain mode.

[-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` .

[-comment <text>] - CIFS Server Description

This optional parameter specifies a text comment for the server. CIFS clients can see this CIFS server description when browsing servers on the network. The comment can be up to 48 characters long. If there is a space in the descriptive remark or the path, you must enclose the entire string in quotation marks.

[-netbios-aliases <NetBIOS>,…] - List of NetBIOS Aliases

This parameter specifies a list of NetBIOS aliases, which are alternate names to the CIFS server name.

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:
```

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER2
-domain EXAMPLE.com -keytab-uri
http://nbsweb.eng.btc.netapp.in/~user/Sample1.keytab
Info: SMB1 protocol version is disabled on this CIFS server. If required,
use
the (privilege: advanced) command "vserver cifs options modify -vserver
vs1
-smb1-enabled true" to enable it.
```

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and workgroup Sales:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and domain EXAMPLE.com with a user Administrator1 from a different domain, in this case an administrator from a trusted domain TRUST.LAB.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: Administrator1@TRUST.LAB.COM

Enter the password:
```

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 with domain EXAMPLE.com using nested OUs:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-domain EXAMPLE.com -ou OU=developers,OU=engineering,OU=corp
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 "OU=developers,OU=engineering,OU=corp"
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. You also can modify the name and ou of the CIFS server, join to a new domain or a workgroup, or rejoin to current domain. When a CIFS server is joining a domain, this command might take several minutes to complete.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver for the CIFS server whose associated site you want to modify.

`[-cifs-server <NetBIOS>]` - CIFS Server NetBIOS Name

This parameter specifies the name of the CIFS server (up to 15 characters). Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify-status-admin` *down* `command. When the command completes successfully, the administrative status of the CIFS server is automatically set to` *up*``.

{ `[-domain <TextNoCase>]` - Fully Qualified Domain Name

This parameter specifies the fully qualified name of the Active Directory domain to associate with the CIFS server. Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify -status-admin` *down* `command. When the command completes successfully, the administrative status of the CIFS server is automatically set to` *up*``.

`[-ou <text>]` - Organizational Unit

This parameter specifies the organization unit within the Active Directory domain to associate with the CIFS server. By default, this parameter is set to CN=Computers. Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify-status-admin` *down* `command. When the command completes successfully, the administrative status of the CIFS server is automatically set to` *up*``. Modifications to this parameter are not supported for workgroup CIFS servers.

`[-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. Modifications to this parameter are not supported for workgroup CIFS servers.

| `[-workgroup <NetBIOS>]` - Workgroup Name }

This parameter specifies the name of the workgroup (up to 15 characters).

[-keytab-uri {(ftp|http)://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Kerberos Keytab File URI (privilege: advanced)

This parameter specifies loading a keytab file from the specified URI. This is applicabe if the CIFS server is being created in realm mode or domain mode.

[-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.

[-comment <text>] - CIFS Server Description

Use this parameter to modify the comment of the server.

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 and ou for the CIFS server associated with Vserver "vs1". The administrative status of the CIFS server must be set to "down" 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 -ou
ou=example_ou -cifs-server example -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 "ou=example_ou" container within the
"example.com"
domain.

Enter the user name: administrator

Enter the password:

cluster1::>
```

The following example modifies the CIFS server associated with Vserver "vs1" from a domain to a workgroup. The administrative status of the CIFS server must be set to "down" for this command. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup Sales -status
-admin down

Warning: To enter workgroup mode, all domain-based features must be
disabled
         and their configuration removed automatically by the system,
         including continuously-available shares, shadow copies, and AES.
         However, domain-configured share ACLs such as
         "EXAMPLE.COM\userName" will not work properly, but cannot be
         removed by Data ONTAP. Remove these share ACLs as soon as
possible
         using external tools after the command completes. If AES is
enabled,
         you may be asked to supply the name and password of a Windows
account
         with sufficient privileges to disable it in the "EXAMPLE.COM"
domain.
Do you want to continue? {y|n}: y

cluster1::>
```

The following example modifies the CIFS server associated with Vserver "vs1" from a workgroup to a domain. The administrative status of the CIFS server must be set to "down" for this command. 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 "ou=example_ou" container within the
"example.com"
domain.

Enter the user name: administrator

Enter the password:

cluster1::>
```

The following example modifies the CIFS server associated with Vserver "vs1" from a workgroup to a domain using keytab-uri. The administrative status of the CIFS server must be set to "down" for this command. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -keytab
-uri http://nbsweb.eng.btc.netapp.in/~shravanp/Sample1.keytab -status
-admin down

cluster1::>
```

The following example modifies the CIFS server name associated with Vserver "vs1" from above example. The administrative status of the CIFS server must be set to "down" to proceed with Active Directory domain modification. If the command completes successfully, the administrative status is automatically set to "up" and there will be a job running to update related configurations.

```
cluster1::> vserver cifs modify -vserver vs1 -cifs-server new_example
-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 "ou=example_ou" container within the
"example.com"
domain.

Enter the user name: administrator

Enter the password:

Successfully queued CIFS Server Modify job [id: xx] for CIFS server
"NEW_EXAMPLE". To view the status of the job, use the "job show -id
<jobid>"
command.

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.

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 prepare-to-downgrade

Restore the CIFS Configurations to Earlier Release of Data ONTAP Version

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

Description

The `vserver cifs prepare-to-downgrade` command restores the CIFS configurations for Data ONTAP based on the input parameter disable-feature-set.

Parameters

`-disable-feature-set <downgrade version>` - Data ONTAP Version (privilege: advanced)

This parameter specifies the Data ONTAP release for which the CIFS configurations are restored. The value can be one of the following:

- 8.3.1 - Restores the CIFS configurations for Data ONTAP release 8.3.1. These features include:
- FPolicy "close with read" filters from FPolicy events.
- CIFS server options `-guest-unix-user` and `-is-admin-users-mapped-to-root-enabled`.
- CIFS security option `is-smb-encryption-required`.
- Storage-Level Access Guard (SLAG) for qtrees.
- CIFS share property `encrypt-data`.
- 8.3.2 - Restores the CIFS configurations for Data ONTAP release 8.3.2. These features include:
- CIFS server option `-grant-unix-group-perms-to-others`.
- 9.0.0 - Restores the CIFS configurations for Data ONTAP release 9.0.0. These features include:
- Disable CIFS multichannel feature and close all multichannel connections.
- Delete all the name-mapping entries that have a hostname or an address field configured.
- Terminate all SMB 3.1 client connections.
- Terminate all client connections that have large MTU negotiated.
- Remove the symlink property `no-strict-security`.
- Remove all symlink pathmap entries with locality `freelink`.

Examples

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 8.3.1
```

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 8.3.2
```

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 9.0.0
```

vserver cifs remove-netbios-aliases

Remove NetBIOS aliases

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

Description

```
The `vserver cifs remove-netbios-aliases` command deletes NetBIOS aliases
for the CIFS server.
```

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver from which the list of NetBIOS aliases are deleted.

-netbios-aliases <NetBIOS>,… - List of NetBIOS Aliases

This parameter specifies one or more NetBIOS aliases to be deleted. To delete all the NetBIOS aliases of a Vserver use '-'.

Examples

The following example deletes NetBIOS aliases for the CIFS server CIFS_SERVER on Vserver vs_a.

```
cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                   ALIAS_5, ALIAS_6, ALIAS_7

cluster1::> cifs remove-netbios-aliases -netbios-aliases
alias_1,alias_3,alias_5

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6, ALIAS_7

cluster1::> cifs remove-netbios-aliases -netbios-aliases alias_7

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6

cluster1::> cifs remove-netbios-aliases -netbios-aliases -

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: -
```

vserver cifs repair-modify

Repair a partially-failed Vserver CIFS server modify operation

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

Description

Use this `vserver cifs repair-modify -vserver <vserver name>` command when the background job created during a Vserver CIFS server modify operation fails.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

This parameter specifies a Vserver containing a configured CIFS server that has been modified.

Examples

The following example starts the CIFS server modify job on Vserver vs1 successfully:

```
cluster1::*> vserver cifs repair-modify -vserver vs1

Successfully queued CIFS Server Modify job [id: 10] for CIFS server
"CIFSNAME1".
To view the status of the job, use the "job show -id <jobid>" command.

cluster1::*>
```

The following example fails the command with specific error:

```
cluster1::*> vserver cifs repair-modify -vserver vs2

Error: Job Out of memory. Failed to queue CIFS Server Modify Job for CIFS
server "CIFSNAME2". Retry the operation by running (privilege: advanced)
"vserver cifs repair-modify -vserver vs2".
Error: command failed: unable to save data

cluster1::*>
```

vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade

Disabled encryption-required-for-dc-connections option and capability for downgrade.

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

Description

The `vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade` prepares the cluster for downgrade by disabling SMB3.encryption.required.dc.connection capability

Examples

```
cluster1::*> vserver cifs security-encryption-required-dc-connections-
prepare-to-downgrade
```

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.

| [-display-netbios-aliases]

If you specify this parameter, the command displays information about configured NetBIOS aliases.

| [-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 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 CIFS server NetBIOS 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.

[-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.

[-ou <text>] - Organizational Unit

If you specify this parameter, the command displays information only for CIFS servers that are in the specified organizational unit.

[-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.

[-workgroup <NetBIOS>] - Workgroup Name

If you specify this parameter, the command displays information only for CIFS servers that are in the specified workgroup.

[-auth-style {domain|workgroup|realm}] - Authentication Style

If you specify this parameter, the command displays information only for CIFS servers that match the specified authentication style.

[-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.

[-comment <text>] - CIFS Server Description

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

[-netbios-aliases <NetBIOS>,…] - List of NetBIOS Aliases

If you specify this parameter, the command displays information only for CIFS servers that have specified NetBIOS alias.

Examples

The following example displays a subset of the information about all CIFS servers:

```
cluster1::> vserver cifs show
Server      Domain/Workgroup
 Vserver        Name        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
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                              Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_2, ALIAS_4,
ALIAS_6
```

The following example displays the NetBIOS aliases for the CIFS server CIFSSERVER1

```
cluster1::> cifs show -display-netbios-aliases

Vserver: vs1
Server Name: CIFSSERVER1
  NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6
```

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
```

Related Links

- 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.

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.

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"
```

Related Links

- 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.

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.

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.

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.

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 vserver 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 vserver 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
```

Related Links

- 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
                Operating  Allowed     Max
 Vserver        Mode       Versions    Size   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
                Operating  Allowed     Max
 Vserver        Mode       Versions    Size   Path
 -------------- ---------- ----------- ------ ------------------------
 vs1            per_share  enable_all     1GB /branchcache_hash_store
```

vserver cifs cache name-to-sid delete-all

Delete all the entries for the vserver

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

Description

The `vserver cifs cache name-to-sid delete-all` command removes all of the Windows user cache entries cached by the Windows name for the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the name-to-sid cache entries need to be deleted.

Examples

The following example shows how to delete all of the cached name-to-sid entries for Vserver vs0:

```
cluster1::> vserver cifs cache name-to-sid delete-all -vserver vs0
```

vserver cifs cache name-to-sid delete

Delete an entry

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

Description

The `vserver cifs cache name-to-sid delete` command removes the Windows user cache entries cached by the Windows name. If cache propagation is enabled, the corresponding sid-to-name cache entry will also be removed.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the name-to-sid cache entry needs to be deleted.

`-win-name <text>` - Windows Name (privilege: advanced)

Use this parameter to specify the Windows name for which the cached entry needs to be deleted.

Examples

The following example shows how to delete the name-to-sid cache entry for Vserver vs0 with Windows name user1:

```
cluster1::> vserver cifs cache name-to-sid delete -vserver vs0 -win-name
user1
```

vserver cifs cache name-to-sid show

Display name-to-sid cache entries

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

Description

The `vserver cifs cache name-to-sid show` command displays the Windows user information cached by Windows 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] }

Use this parameter to display detailed information about the Windows user entries cached by the Windows name.

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

Use this parameter to specify the Vserver for which the Windows user entries that are cached by the Windows name need to be displayed.

[-win-name <text>] - Windows Name (privilege: advanced)

Use this parameter to specify the Windows name for which the cached entries need to be displayed.

[-sid <text>] - SID (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID).

[-sid-type <integer>] - SID type (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) type.

[-flags <integer>] - Flags (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the Windows name that have the specified flags.

[-domain-name <text>] - Domain Name (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the Windows name that have the specified domain name.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the Windows user entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the user entries cached by the Windows name that have the specified lookup source.

Examples

The following example shows how to display all of the Windows users which are cached by the Windows name:

```
cluster1::> vserver cifs cache name-to-sid show
```

The following example shows how to display all of the Windows user entries cached by the Windows name for Vserver vs0:

```
cluster1::> vserver cifs cache name-to-sid show -vserver vs0
```

vserver cifs cache settings modify

Modify CIFS Cache Configuration

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

Description

The `vserver cifs cache settings modify` command modifies the Windows users cache configuration of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the Windows users cache settings need to be modified.

`[-is-enabled {true|false}]` - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the Windows users database. The value *`true`* means the cache is enabled and the value *`false`* means the cache is disabled. The default value for this parameter is *`false`* .

`[-is-negative-cache-enabled {true|false}]` - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the Windows users database and the look-up fails. The default value for this parameter is *`true`* . Negative cache is disabled by default if the parameter *`is-enabled`* is set to *`false`* .

`[-ttl <[<integer>h][<integer>m][<integer>s]>]` - Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes, and seconds) for which the positive entries need to be cached. The positive entries means the entries which are present in the Windows users database and the look-up succeeds. The default value is 24 hours.

`[-negative-ttl <[<integer>h][<integer>m][<integer>s]>]` - Negative Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes, and seconds) for which the negative entries need to be cached. The default value is 5 minutes.

`[-is-propagation-enabled {true|false}]` - Is Propagation Enabled? (privilege: advanced)

Use this parameter to specify whether the cached user entries need to be propagated to the sid-to-name cache. The default value is *`true`* . Specify *`false`* to disable propagation.

Examples

The following example shows how to modify the Windows users cache configuration settings for Vserver vs0:

```
cluster1::> vserver cifs cache settings modify -vserver vs0 -ttl 600
-negative-ttl 300
```

The following example shows how to disable the Windows users cache for Vserver vs0:

```
cluster1::> vserver cifs cache settings modify -vserver vs0 -is-enabled
false
```

vserver cifs cache settings show

Display CIFS Cache Configuration

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

Description

The `vserver cifs cache settings show` command displays information about the Windows users cache configuration of the 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] }

Use this parameter to display detailed information about the Windows users cache configuration settings.

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

Use this parameter to display information about the Windows users cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the Windows users cache configuration settings that have the specified cache enabled setting. Value *`true`* displays only the entries that have cache enabled and value *`false`* displays only the entries that have cache disabled.

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the Windows users cache configuration settings that have the specified negative cache enabled setting. Value *`true`* displays only the entries that have negative cache enabled and value *`false`* displays only the entries that have negative cache disabled.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to display information only about the Windows users cache configuration settings that have the specified Time to Live.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to display information only about the Windows users cache configuration settings that have the specified negative Time to Live.

[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)

Use this parameter to display information only about the Windows users cache configuration settings that have the specified propagation enabled setting. Value *true* displays only the entries that have the propagation of cached entries to sid-to-name cache enabled and value *false* displays only the entries that have the propagation of cached entries to sid-to-name cache disabled.

Examples

The following example shows how to display the Windows users cache configuration settings for all the Vservers:

```
cluster1::> vserver cifs cache settings show
```

The following example shows how to display the Windows users cache configuration settings for Vserver vs0:

```
cluster1::> vserver cifs cache settings show -vserver vs0
```

The following example shows how to display the Windows users cache configuration settings that have cache disabled:

```
cluster1::> vserver cifs cache settings show -is-enabled false
```

vserver cifs cache sid-to-name delete-all

Delete all the entries for the vserver

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

Description

The `vserver cifs cache sid-to-name delete-all` command removes all of the Windows user cache entries cached by the security identifier (SID) for the specified Vserver.

Parameters

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

Use this parameter to specify the Vserver for which the sid-to-name cache entries need to be deleted.

Examples

The following example shows how to delete all the cached sid-to-name entries for Vserver vs0:

```
cluster1::> vserver cifs cache sid-to-name delete-all -vserver vs0
```

vserver cifs cache sid-to-name delete

Delete an entry

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

Description

The `vserver cifs cache sid-to-name delete` command removes the Windows user cache entries cached by security identifier (SID). If cache propagation is enabled, the corresponding name-to-sid cache entry will also be removed.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the sid-to-name cache entry needs to be deleted.

`-sid <text>` - SID (privilege: advanced)

Use this parameter to specify the security identifier (SID) for which the cached entry needs to be deleted.

Examples

The following example shows how to delete the sid-to-name cache entry for Vserver vs0 with SID S-1-5-21-1380078113-1824080971-954447143-1152:

```
cluster1::> vserver cifs cache sid-to-name delete -vserver vs0 -sid S-1-5-
21-1380078113-1824080971-954447143-1152
```

vserver cifs cache sid-to-name show

Display sid-to-name cache entries

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

Description

The `vserver cifs cache sid-to-name show` command displays the Windows user information cached by security identifier (SID).

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] }

Use this parameter to display detailed information about the Windows user entries cached by the security identifier (SID).

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

Use this parameter to specify the Vserver for which the Windows user entries that are cached by the security identifier (SID) need to be displayed.

[-sid <text>] - SID (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID).

[-win-name <text>] - Windows Name (privilege: advanced)

Use this parameter to specify the Windows name for which the cached entries need to be displayed.

[-sid-type <integer>] - SID type (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) type.

[-sid-mode <integer>] - SID mode (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) mode.

[-flags <integer>] - Flags (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified flags.

[-domain-name <text>] - Domain Name (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified domain name.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the Windows user entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified lookup source.

Examples

The following example shows how to display all of the Windows users which are cached by the security identifier (SID):

```
cluster1::> vserver cifs cache sid-to-name show
```

The following example shows how to display all of the Windows user entries cached by the security identifier (SID) for Vserver vs0:

```
cluster1::> vserver cifs cache sid-to-name show -vserver vs0
```

vserver cifs character-mapping create

Create character mapping on a volume

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

Description

The `vserver cifs character-mapping create` command creates the CIFS character mapping for the specified volume on a particular Vserver.

> Choose target characters in the "Private Use Area" of Unicode in the following range: U+E0000…U+F8FF.

> The target Unicode characters must not appear in existing file names; otherwise, unwanted character mappings would occur, resulting in clients being unable to access mapped files. For example, if ":" is mapped to "-" but "-" appears in files normally, a Windows client using the mapped share to access a file named "a-b" would have its request mapped to the NFS name "a:b", which is not the desired file.

The `vserver cifs character-mapping create` command is not supported for FlexGroups.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which a volume is located for which you are creating the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

`-volume <volume name>` - Volume Name

This parameter specifies the name of the volume for which you are creating the character mapping.

`-mapping <text>,…` - Character Mapping

This parameter specifies the mapping of the invalid CIFS filename characters to valid CIFS filename characters. The mapping consists of a list of source-target character pairs separated by ":". The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

> The permissible Unicode character set for source mapping is: 0x01-0x19, 0x5C, 0x3A, 0x2A, 0x3F, 0x22, 0x3C, 0x3E, 0x7C, 0xB1.

Examples

The following example creates a character mapping for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping create -volume vol1 -mapping
3c:e17c, 3e:f17d, 2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             vol1         3c:e17c, 3e:f17d, 2a:f745
```

vserver cifs character-mapping delete

Delete character mapping on a volume

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

Description

The `vserver cifs character-mapping delete` command deletes the CIFS character mapping for the specified volume on a particular Vserver.

The `vserver cifs character-mapping delete` command is not supported for FlexGroups.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which a Volume is located for which you are deleting the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

`-volume <volume name>` - Volume Name

This parameter specifies the name of the volume for which you are deleting the character mapping.

Examples

The following example deletes all character mappings for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping delete -volume vol1
```

vserver cifs character-mapping modify

Modify character mapping on a volume

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

Description

The `vserver cifs character-mapping modify` command modifies the CIFS character mapping for the specified volume on a particular Vserver.

You can modify a particular volume's character mapping by specifying the following two parameters in the

modify command:

- Vserver associated with the volume
- Name of the Volume

Choose target characters in the "Private Use Area" of Unicode in the following range: U+E0000…U+F8FF.

The target Unicode characters must not appear in existing file names; otherwise, unwanted character mappings would occur, resulting in clients being unable to access mapped files. For example, if ":" is mapped to "-" but "-" appears in files normally, a Windows client using the mapped share to access a file named "a-b" would have its request mapped to the NFS name "a:b", which is not the desired file.

The `vserver cifs character-mapping modify` command is not supported for FlexGroups.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which a Volume is located for which you are modifying the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

`-volume <volume name>` - Volume Name

This parameter specifies the name of the volume for which you are modifying the character mapping.

`[-mapping <text>,…]` - Character Mapping

This parameter specifies the mapping of the invalid CIFS filename characters to valid CIFS filename characters. The mapping consists of a list of source-target character pairs separated by ":". The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

The permissible Unicode character set for source mapping is: 0x01-0x19, 0x5C, 0x3A, 0x2A, 0x3F, 0x22, 0x3C, 0x3E, 0x7C, 0xB1.

Examples

The following example modifies a character mapping for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping modify -volume vol1 -mapping
3c:e17d, 3e:f17e, 2a:f746
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             vol1         3c:e17d, 3e:f17e, 2a:f746
```

vserver cifs character-mapping show

Display character mapping on volumes

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

Description

The `vserver cifs character-mapping show` command displays information about character mapping configured for volumes. 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 character mapping configured for volumes:

- Vserver name
- Volume name
- Character mapping

Parameters

{ [-fields <fieldname>,…]

If you specify this 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 about character mapping configured for all the volumes that belong to the specified Vserver.

[-volume <volume name>] - Volume Name

If you specify this parameter, the command displays information about the character mapping configured for all the volumes that match the specified volume name.

[-mapping <text>,…] - Character Mapping

If you specify this parameter, the command displays information about the character mapping configured for all volumes that match the specified mapping.

Examples

The following example displays information about all character mappings configured for volumes

```
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             vol1         3c:e17d, 3e:f17e
```

vserver cifs connection show

Displays established CIFS connections

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

Description

The `vserver cifs connection show` command displays information about established CIFS connections.

Parameters

{ [-fields <fieldname>,…]

Use this parameter to display only the specified fields

| [-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 about CIFS connections on the specified node.

[-vserver <vserver name>] - Vserver

Use this parameter to display information about CIFS connections on the specified CIFS-enabled SVM.

[-connection-id <integer>] - Connection ID

Use this parameter to display information about CIFS connections that match the specified connection ID.

[-session-id <integer>,…] - Session ID

Use this parameter to display information about CIFS connections that match the specified session ID.

[-workstation-ip <IP Address>] - Workstation IP Address

Use this parameter to display information about CIFS connections that are established through the specified data LIF IP address.

[-workstation-port <integer>] - Workstation Port Number

Use this parameter to display information about CIFS connections that are opened from the specified Port number.

[-lif-ip <IP Address>] - Incoming Data LIF IP Address

Use this parameter to display information about CIFS connections that are opened from the specified IP address.

[-network-context-id <integer>] - Network Context ID (privilege: advanced)

Use this parameter to display information about CIFS connections that match the specified network context ID.

Examples

The following example displays information about all CIFS connections:

```
cluster1::> vserver cifs connection show
Node:    node1
Vserver: vs1
Connection Session                          Workstation
ID         IDs                Workstation IP Port        LIF IP
---------- ------------------ -------------- ----------- -----------
127834     1,2                172.17.193.172 15536       10.53.50.42
```

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}] - 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.

[-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.

[-preference {unknown|preferred|favored|adequate}] - Preference

If you use this parameter, the command only displays servers of the specified preference level.

[-status {OK|unavailable|slow|expired|undetermined|unreachable}] - Status

If you use this parameter, the command only displays servers of the specified status.

[-dc-functional-level {win2000|unknown|win2003|win2008|win2008r2|win2012|win2012r2|win2016|winthreshold}] - DC Functional Level

If you use this parameter, the command only displays servers with the specified functional level.

[-is-dc-read-only {true|false}] - Is DC Read Only

If this parameter is set to true, the command only displays servers with read only domain controller. If set to false, the command only displays servers with writable domain controller.

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 discovered-servers discovery-mode modify

Modify Server Discovery Mode

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

Description

The `vserver cifs domain discovered-servers discovery-mode modify` command modifies the configuration for the server discovery mode of one or more Data Vservers.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which you want to modify the server discovery mode.

`[-mode {all|site|none}]` - Server Discovery Mode (privilege: advanced)

Use this parameter to specify the server discovery mode for the Vserver. Following are the possible values for this parameter:

- all - Discover all the servers in the domain (default).
- site - Discover the servers local to the site.
- none - Discover nothing. Depend only on preferred-dc configured.

Examples

The following example disables server discovery for a Vserver.

```
cluster1::> vserver cifs domain discovered-servers discovery-mode modify
-vserver vs1 -mode none
```

vserver cifs domain discovered-servers discovery-mode show

Display Server Discovery Mode

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

Description

The `vserver cifs domain discovered-servers discovery-mode show` command displays information about the discovery mode servers for the CIFS domains of 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 (privilege: advanced)

If you use this parameter, the command only displays discovery mode for the specified Vserver.

[-mode {all|site|none}] - Server Discovery Mode (privilege: advanced)

If you use this parameter, the command only displays Vservers with the specified mode.

Examples

The following example shows the server discovery mode for all Vservers.

```
cluster1::> vserver cifs domain discovered-servers discovery-mode show
Vserver         Mode
--------------- ----------
vs1             all
vs2             site
vs3             none
3 entries were displayed.
```

vserver cifs domain name-mapping-search add

Add to the list of trusted domains for name-mapping

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

Description

The `vserver cifs domain name-mapping-search add` command adds one or more trusted domains to the list of trusted domains to be used in preference to all others by the specified Vserver for looking up Windows user names when performing Windows user to UNIX user name-mapping. If a list already exists for

the specified vserver, the new list is merged with the existing list. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for which you want to add trusted domains.

`-trusted-domains <domain name>,…` - Trusted Domains

This parameter specifies a comma-delimited list of fully-qualified domain names of the trusted domains for the home domain.

Examples

The following example adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred list used by Vserver vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

vserver cifs domain name-mapping-search modify

Modify the list of trusted domains for name-mapping search

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

Description

The `vserver cifs domain name-mapping-search modify` command modifies the current list of trusted domains to be used in preference to all others by the specified Vserver to lookup Windows user names when performing Windows user to UNIX user name-mapping. The new list overwrites the existing list. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for which you want to modify the trusted domain list.

`-trusted-domains <domain name>,…` - Trusted Domains

This parameter specifies a comma-delimited list of fully qualified domain names of the trusted domains of the home domain.

Examples

The following example modifies the trusted domain list used by Vserver vs1:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

vserver cifs domain name-mapping-search remove

Remove from the list of trusted domains for name-mapping search

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

Description

The `vserver cifs domain name-mapping-search remove` command removes one or more trusted domains from the list used by the specified Vserver to lookup Windows user names when performing Windows user to UNIX user name-mapping. If a list of trusted domains is not provided, the entire trusted domain list for the specified Vserver is removed. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver from which you want to remove trusted domains.

`[-trusted-domains <domain name>,…]` - Trusted Domains

This parameter specifies a comma-delimited list of trusted domains of the home domain.

Examples

The following example removes two trusted domains from the list used by Vserver vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -trusted
-domains cifs1.example.com, cifs2.example.com
```

vserver cifs domain name-mapping-search show

Display the list of trusted domains for name-mapping searches

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

Description

The `vserver cifs domain name-mapping-search show` command displays information about trusted domains of the home domain by 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

This parameter specifies the name of the Vserver for which you want to display information about the trusted domains.

[-trusted-domains <domain name>,…] - Trusted domains

This parameter specifies a comma-delimited list of fully qualified domain names of trusted domains for which you want to display information.

Examples

The following example displays information about all preferred trusted domains:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vserver_1       CIFS1.EXAMPLE.COM
```

vserver cifs domain password change

Generate a new password for the CIFS server's machine account and change it in the Windows Active Directory domain.

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

Description

The `vserver cifs domain password change` changes the domain account password for a CIFS server. This command is not supported for workgroup CIFS servers.

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 domain password change -vserver vs1

cluster1::>
```

vserver cifs domain password reset

Reset the CIFS server's machine account password in the Windows Active Directory domain.

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

Description

The `vserver cifs domain 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. This command is not supported for workgroup CIFS servers.

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 domain password reset -vserver vs1

Enter your user ID: Administrator
Enter your password:

cluster1::>
```

vserver cifs domain password schedule modify

Modify the domain account password change schedule

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

Description

The `vserver cifs domain password schedule modify` command enables you to modify a domain account password change schedule for a CIFS server. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver

This specifies the name of the Vserver containing the CIFS server for which you want to change the domain account password.

`[-is-schedule-enabled {true|false}]` - Is Password Change Schedule Enabled

This specifies whether the domain account password change schedule is enabled.

[-schedule-weekly-interval <integer>] - Interval in Weeks for Password Change Schedule

This specifies the number of weeks after which the scheduled domain account password change must occur.

[-schedule-randomized-minute <integer>] - Minutes Within Which Schedule Start Can be Randomized

This specifies the minutes within which the scheduled domain account password change must begin.

[-schedule-day-of-week <cron_dayofweek>] - Day of Week for Password Change Schedule

This sets the day of week when the scheduled domain account password change occurs.

[-schedule-time-of-day <HH:MM:SS>] - Start Time for Password Change Schedule

This sets the time in HH:MM:SS at which the scheduled domain account password change starts.

Examples

The following example enables the domain account password change schedule and configures it to run at any time between 23:00:00 to 00:59:00 (one hour before midnight to one hour after midnight) on every 4th Sunday.

```
cluster1::> vserver cifs domain password schedule modify -is-schedule
-enabled true -schedule-randomized-minute 120 -schedule-weekly-interval 4
-schedule-time-of-day 23:00:00 -schedule-day-of-week sunday
```

vserver cifs domain password schedule show

Display the domain account password change schedule

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

Description

The `vserver cifs domain password schedule show` command displays the domain account password change schedule configuration. It displays the following fields:

- Vserver: Vserver for which the schedule is configured
- Schedule Enabled: Whether the schedule is enabled or disabled for this Vserver
- Schedule Interval: Weeks after which the password change schedule occurs again for this Vserver
- Schedule Randomized Within: Minutes within which the schedule must begin for this Vserver
- Schedule: Password change schedule currently set on this Vserver
- Last Successful Password Change/Reset Time: Time at which the last password change or reset happened successfully on this Vserver
- Warning: Warning message, applicable only when the change password job is deleted with the feature still enabled on this 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

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

[-is-schedule-enabled {true|false}] - Is Password Change Schedule Enabled

If you specify this parameter, the command displays information for all the Vservers on which the is-schedule-enabled value applies.

[-schedule-weekly-interval <integer>] - Interval in Weeks for Password Change Schedule

If you specify this parameter, the command displays information for all the Vservers on which the schedule-weekly-interval value applies.

[-schedule-randomized-minute <integer>] - Minutes Within Which Schedule Start Can be Randomized

If you specify this parameter, the command displays information for all the Vservers on which the schedule-randomized-minute value applies.

[-schedule-last-changed <text>] - Last Successful Password Change/Reset Time

If you specify this parameter, the command displays information for all the Vservers on which the schedule-last-changed value applies.

[-schedule-description <text>] - Schedule Description

If you specify this parameter, the command displays information for all the Vservers on which the schedule-description value applies.

[-schedule-warn-msg <text>] - Warning Message in Case Job Is Deleted

If you specify this parameter, the command displays information for all the Vservers on which the schedule-warn-msg value applies.

Examples

The following example shows the domain account password change schedule configuration when the password change feature is enabled for Vserver vs1.

```
cluster1::> vserver cifs domain password schedule show
Vserver: vs1
Schedule Enabled: true
            Schedule Interval: 4   week
   Schedule Randomized Within: 120 min
                     Schedule: Fri@23:00
              Last Changed At: Thu Apr  4 02:35:23 2013
```

The following example shows the domain account password change schedule configuration when the password change job has been accidently deleted.

```
cluster1::> vserver cifs domain password schedule show
Vserver: vs1
Schedule Enabled: true
            Schedule Interval: 4   week
   Schedule Randomized Within: 120 min
                     Schedule: Fri@23:00
              Last Changed At: Thu Apr  4 02:35:23 2013
                      Warning: Password change job was deleted. Re-enable
the password change schedule.
```

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. This command is not supported for workgroup CIFS servers.

> 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.

`[-skip-config-validation <true>]` - Skip Configuration Validation

Use this parameter to skip the Preferred-DC configuration validation.

The hosts specified with the `-DC-servers` parameter are validated to verify that each of the DC servers are reachable, and is providing NETLOGON services.

The validation fails if there is no valid Preferred-DC server.

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 check

Display validation status of the Preferred-DC configuration

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

Description

Use the `vserver cifs domain preferred-dc check` command to check the status of configured preferred DC on a particular 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> - Vserver

Use this parameter to specify the Vserver whose preferred DC needs to be validated.

[-server-ip <text>,…] - DC Address

Use this parameter to display IP-address of the configured CIFS Preferred-DC servers.

[-domain <TextNoCase>,…] - Domain Name

Use this parameter to display Domain name of the configured CIFS Preferred-DCs.

[-status {down|up}] - DC Status

Use this parameter to display information only about CIFS Preferred-DC servers with a status that matches the value you specify.

[-status-details <text>,…] - Status Details

Use this parameter to display information only about CIFS Preferred-DC servers with status details that match the value you specify.

Examples

The following example checks the connectivity of preferred DC on vserver vs0.

```
cluster1::> vserver cifs domain preferred-dc check -vserver vs0

Vserver : vs0

Domain Name             DC Address          Status       Status Details
-----------             -----------         ------       --------------
example.com             1.1.1.1              up         Response time
(msec): 426
example.com             1.1.1.2              up         Response time
(msec): 425
example1.com            2.2.2.2              up         Response time
(msec): 423
example2.com            3.3.3.3              up         Response time
(msec): 422
```

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. This command is not supported for workgroup CIFS servers.

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 domain trusts rediscover

Reset and rediscover trusted domains for a Vserver

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

Description

The `vserver cifs domain trusts rediscover` command discards information the Vserver has stored about trusted domains. After that, it begins the discovery process to reacquire current information about trusted domains. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver.

Examples

The following example rediscovers trusted domains. It produces no output.

```
cluster1::> vserver cifs domain trusts rediscover
```

vserver cifs domain trusts show

Display discovered trusted domain information

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

Description

The `vserver cifs domain trusts show` command displays information about the trusted domains for the CIFS home domain of one or more Vservers. The displayed trusted domain information is grouped by node and Vserver, and each group is preceded by the node and Vserver identification. This command is not supported for workgroup CIFS servers.

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 displays information only about trusted domains of the home domains for the specified node.

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

If you use this parameter, the command displays information only about trusted domains of the home domain for the specified Vserver.

[-home-domain <domain name>] - Home Domain Name

If you use this parameter, the command displays information only about trusted domains of the home domain with the specified name.

[-trusted-domain <domain name>,…] - Trusted Domain Name

If you use this parameter, the command displays information only about trusted domains with the specified name.

Examples

The following example displays information about all the bidirectional trusted domains for node-01 and vserver_1.

```
cluster1::> vserver cifs domain trusts show -node node-01 -vserver
vserver_1
Node: node-01
Vserver: vserver_1

Home Domain            Trusted Domain
---------------------  ----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
```

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 the group policy configuration of a CIFS server. This command is not supported for workgroup CIFS servers.

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.

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 only group policy information that has been applied to the Vserver you specify.

[-gpo-index <integer>] - GPO Index

If you specify this parameter, the command displays only group policy information at gpo-index.

Examples

The following example displays all group policy information about all group policies that have been applied to a Vserver:

```
cluster1::> vserver cifs group-policy show-applied

Vserver: vs1
 ----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
```

```
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
```

```
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
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.

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 only group policy information that has been defined in Active Directory for the Vserver that you specify.

[-gpo-index <integer>] - GPO Index

If you specify this parameter, the command displays only group policy information at gpo-index.

Examples

The following example displays all group policy information for all group policies that have been defined in Active Directory:

```
cluster1::> vserver cifs group-policy show-defined
```

```
Vserver: vs1
 ----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
```

```
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

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 the group-policy settings defined in Active Directory for the given Vserver. This command is not supported for workgroup CIFS servers.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the CIFS-enabled Vserver to which the group-policy settings be applied.

[-force-reapply-all-settings {true|false}] - Force Re-apply All Settings

This parameter specifies whether to ignore all processing optimizations and re-apply all settings. The default is false.

Examples

The following example applies the group-policy settings defined in Active Directory for Vserver vs1.

```
cluster1::> vserver cifs group-policy update -vserver vs1 -force-reapply
-all-settings true
```

vserver cifs group-policy central-access-policy show-applied

Show currently applied central access policies

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

Description

The `vserver cifs group-policy central-access-policy show-applied` command displays information about the central access policies assigned to 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 CIFS servers:

- Vserver name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

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 for central access policies for the specified Vserver.

[-name <TextNoCase>] - Name

If you specify this parameter, the command displays information only for central access policies that match the specified name.

[-sid <windows sid>] - Identifier

If you specify this parameter, the command displays information only for central access policies that match the specified SID.

[-description <text>] - Description

If you specify this parameter, the command displays information only for central access policies that match the specified description.

[-ctime <Date>] - Creation Time

If you specify this parameter, the command displays information only for central access policies that match the specified creation time.

[-mtime <Date>] - Modification Time

If you specify this parameter, the command displays information only for central access policies that match the specified modification time.

[-rules <TextNoCase>,…] - Central Access Rules

If you specify this parameter, the command displays information only for central access policies that match the specified member rules.

Examples

The following example displays information for all central access policies:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
---------- --------------------
-----------------------------------------------
vs1        p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
        Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
  Modification Time: Wed Oct 23 08:59:15 2013
       Member Rules: r1

vs1        p2                   S-1-17-1885229282-1100162114-134354072-
822349040
        Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
  Modification Time: Thu Oct 31 10:25:32 2013
       Member Rules: r1
                     r2

2 entries were displayed.
```

vserver cifs group-policy central-access-policy show-defined

Show applicable central access policies defined in the Active Directory

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

Description

The `vserver cifs group-policy central-access-policy show-defined` command displays information about the central access policies that are defined in the Active Directory. 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
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

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 for central access policies for the specified Vserver.

[-name <TextNoCase>] - Name

If you specify this parameter, the command displays information only for central access policies that match the specified name.

[-sid <windows sid>] - Identifier

If you specify this parameter, the command displays information only for central access policies that match the specified SID.

[-description <text>] - Description

If you specify this parameter, the command displays information only for central access policies that match the specified description.

[-ctime <Date>] - Creation Time

If you specify this parameter, the command displays information only for central access policies that match the specified creation time.

[-mtime <Date>] - Modification Time

If you specify this parameter, the command displays information only for central access policies that match the specified modification time.

[-rules <TextNoCase>,…] - Central Access Rules

If you specify this parameter, the command displays information only for central access policies that match the specified member rules.

Examples

The following example displays information for all central access policies:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver    Name                 SID
---------- --------------------
-------------------------------------------
vs1        p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
        Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
  Modification Time: Wed Oct 23 08:59:15 2013
       Member Rules: r1

vs1        p2                   S-1-17-1885229282-1100162114-134354072-
822349040
        Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
  Modification Time: Thu Oct 31 10:25:32 2013
       Member Rules: r1
                     r2

2 entries were displayed.
```

vserver cifs group-policy central-access-rule show-applied

Show currently applied central access rules

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

Description

The `vserver cifs group-policy central-access-rule show-applied` command displays information about the central access rules assigned to 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 CIFS servers:

- Vserver name

- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

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 for central access rules for the specified Vserver.

[-name <TextNoCase>] - Name

If you specify this parameter, the command displays information only for central access rules that match the specified name.

[-description <text>] - Description

If you specify this parameter, the command displays information only for central access rules that match the specified description.

[-ctime <Date>] - Creation Time

If you specify this parameter, the command displays information only for central access rules that match the specified creation time.

[-mtime <Date>] - Modification Time

If you specify this parameter, the command displays information only for central access rules that match the specified modification time.

[-effective <text>] - Effective Security Policy

If you specify this parameter, the command displays information only for central access rules that match the specified effective security policy.

[-proposed <text>] - Proposed Security Policy

If you specify this parameter, the command displays information only for central access rules that match the specified proposed security policy.

[-resource <text>] - Resource Condition

If you specify this parameter, the command displays information only for central access rules that match the specified resource condition.

Examples

The following example displays information for all central access rules:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

2 entries were displayed.
```

vserver cifs group-policy central-access-rule show-defined

Show applicable central access rules defined in the Active Directory

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

Description

The `vserver cifs group-policy central-access-rule show-defined` command displays information about the central access rules that are defined in the Active Directory. 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
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

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 for central access rules for the specified Vserver.

[-name <TextNoCase>] - Name

If you specify this parameter, the command displays information only for central access rules that match the specified name.

[-description <text>] - Description

If you specify this parameter, the command displays information only for central access rules that match the specified description.

[-ctime <Date>] - Creation Time

If you specify this parameter, the command displays information only for central access rules that match the specified creation time.

[-mtime <Date>] - Modification Time

If you specify this parameter, the command displays information only for central access rules that match the specified modification time.

[-effective <text>] - Effective Security Policy

If you specify this parameter, the command displays information only for central access rules that match the specified effective security policy.

[-proposed <text>] - Proposed Security Policy

If you specify this parameter, the command displays information only for central access rules that match the specified proposed security policy.

[-resource <text>] - Resource Condition

If you specify this parameter, the command displays information only for central access rules that match the specified resource condition.

Examples

The following example displays information for all central access rules:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

2 entries were displayed.
```

vserver cifs group-policy restricted-group show-applied

Show the applied restricted-group settings.

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

Description

The `vserver cifs group-policy restricted-group show-applied` command displays settings of all the restricted groups applied to a Vserver.

If you do not specify any parameters, the command displays the following information about all the restricted groups applied to all the Vservers in the cluster.

- Group Policy Name: Specifies the name of the group policy.
- Version: Specifies the version of the group policy.
- Link: Specifies the level in which the group policy is configured. Possible values are:
- Local: Group policy is configured in Data ONTAP.
- Site: Group policy is configured at the site level in the Domain Controller.
- Domain: Group policy is configured at the domain level in the Domain Controller.
- OrganizationalUnit: Group policy is configured at the OU level in the Domain controller.
- RSOP: Resultant set of policies derived from all the group policies defined at various levels.
- Group Name: Specifies the name of a restricted group.
- Members: Specifies users and groups who belong to and who do not belong to the restricted group.

- MemberOf: Specifies list of groups to which the restricted group is added. A group can be a member of groups other than the groups listed here.

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 the restricted-group information that has been applied to the specified Vserver.

[-index <integer>] - Index

If this parameter is specified, the command displays the specified index for the group policy in the restricted group. The restricted-group information for the group policy at the specified index.

[-group-name <text>] - Group Name

If this parameter is specified, the command displays the restricted-group information for the specified group name.

[-group-policy-name <text>] - Group Policy Name

If this parameter is specified, the command displays the restricted-group information for the specified group policy name.

[-uuid <UUID>] - UUID

If this parameter is specified, the command displays the restricted-group information for the specified UUID of the group policy.

[-version <integer>] - Version

If this parameter is specified, the command displays the restricted-group information for the specified version of the group policy.

[-link {Local|Site|Domain|OrganizationalUnit|RSOP}] - Link Type

If this parameter is specified, the command displays the restricted-group information for the specified link for the group policy.

[-members <gpoUserGroup>,…] - Members, List of Users/groups

If this parameter is specified, the command displays the restricted-group information for the specified members of users and groups.

[-member-of <gpoUserGroup>,…] - MemberOf, List of Groups

If this parameter is specified, the command displays the restricted-group information for the specified member of the group.

Examples

The following example displays information about all restricted groups that have been applied to a Vserver.

```
cluster1::> vserver cifs group-policy restricted-group show-applied

Vserver: vs_1
 -------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: grp1
               Members: usr1
              MemberOf: GPO\g9
Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: grp1
               Members: usr1
              MemberOf: GPO\g9
```

vserver cifs group-policy restricted-group show-defined

Show the defined restricted-group settings.

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

Description

The `vserver cifs group-policy restricted-group show-defined` command displays settings of all the restricted groups defined in Domain Controller for a Vserver.

If you do not specify any parameters, the command displays the following information about all the restricted groups defined in Domain Controller for all the Vservers in the cluster.

- Group Policy Name: Specifies the name of the group policy.
- Version: Specifies the version of the group policy.
- Link: Specifies the level in which the group policy is configured. Possible values are:
- Local: Group policy is configured in Data ONTAP.
- Site: Group policy is configured at the site level in the Domain Controller.
- Domain: Group policy is configured at the domain level in the Domain Controller.
- OrganizationalUnit: Group policy is configured at the OU level in the Domain Controller.
- RSOP: Resultant set of policies derived from all the group policies defined at various levels.
- Group Name: Specifies the name of a restricted group.

- Members: Specifies users and groups who belong to and who do not belong to the restricted group.
- MemberOf: Specifies list of groups to which the restricted group is added. A group can be a member of groups other than the groups listed here.

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 the restricted-group information that is defeined in Domain Controller for the specified Vserver.

[-index <integer>] - Index

If this parameter is specified, the command displays the specified index for the group policy in the restricted group. The restricted-group information for the group policy at the specified index.

[-group-name <text>] - Group Name

If this parameter is specified, the command displays the restricted-group information for the specified group name.

[-group-policy-name <text>] - Group Policy Name

If this parameter is specified, the command displays the restricted-group information for the specified group policy name.

[-uuid <UUID>] - UUID

If this parameter is specified, the command displays the restricted-group information for the specified UUID of the group policy.

[-version <integer>] - Version

If this parameter is specified, the command displays the restricted-group information for the specified version of the group policy.

[-link {Local|Site|Domain|OrganizationalUnit|RSOP}] - Link Type

If this parameter is specified, the command displays the restricted-group information for the specified link for the group policy.

[-members <gpoUserGroup>,…] - Members, List of Users/groups

If this parameter is specified, the command displays the restricted-group information for the specified members of users and groups.

[-member-of <gpoUserGroup>,…] - MemberOf, List of Groups

If this parameter is specified, the command displays the restricted-group information for the specified member of the group.

Examples

The following example displays information about all restricted groups that are defined in Domain Controller for a Vserver.

```
cluster1::> vserver cifs group-policy restricted-group show-defined

Vserver: vs_1
 -------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: grp1
               Members: usr1
              MemberOf: GPO\g9
Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: grp1
               Members: usr1
              MemberOf: GPO\g9
```

vserver cifs home-directory modify

Modify attributes of CIFS home directories

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

Description

The `vserver cifs home-directory modify` command modifies the CIFS home directory configuration for a CIFS server. To use the home directory option (-is-home-dirs-access-for-admin-enabled), a home directory share must be configured with a dynamic share pattern preceded by a tilde(~). Valid dynamic share patterns are ~%w and ~%d%w. The pattern %u is not supported with the option .

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the name of the CIFS server for which you want to modify the CIFS home directory configuration.

`[-is-home-dirs-access-for-admin-enabled {true|false}]` - Is Home Directory Access for Admin Enabled

This optional parameter specifies whether a user with Windows administrative privileges can connect to another user's home directory. The default value for this parameter is *`true`* .

[-is-home-dirs-access-for-public-enabled {true|false}] - Is Home Directory Access for Public Enabled (privilege: advanced)

This optional parameter specifies whether any user can connect to another user's home directory. The default value for this parameter is *false* .

Examples

The following example modifies the CIFS home directory configuration for the Vserver "vs1". It enables users with Windows administrative privileges to connect to another user's home directory .

```
cluster1::> vserver cifs home-directory modify -vserver vs1 -is-home-dirs
-access-for-admin-enabled true
```

The following example shows the usage of the share creation pattern %d%w.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name ~%d~%w
-path %d/%w -share-properties homedirectory
```

The following example shows the usage of the share creation pattern ~%w.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name ~%w -path
%d/%w -share-properties homedirectory
```

vserver cifs home-directory show-user

Display the Home Directory Path for a User

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

Description

The `vserver cifs home-directory show-user` command prints the path of a user's CIFS home directory. Use this command if multiple CIFS home directory paths exist and you want to see which path holds the user's CIFS home directory.

Parameters

{ [-fields <fieldname>,…]

If you specify this 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> - Vserver

Use this required parameter to specify the Vserver that contains the home directory of the user specified with the required `-username` parameter.

-username <text> - User Name

Use this required parameter to locate the home directory of the specified user. You must enter this parameter in the following format: user, domain/user or cifs_server_name/user.

[-path <text>] - Path

If you specify this parameter, the command displays information about the user's home directory with the specified path.

[-share-name <text>] - Share Name

If you specify this parameter, the command displays information about the user's home directory with the specified home-directory share.

Examples

The following command displays information about the home directory of user gpo\rpuser1 belonging to Vserver vs1.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1
Vserver  : vs1
    Username : GPO/rpuser1
ShareName                                  Home Dir Path
    -----------------------------------
---------------------------------
    root                                       /home/rpuser1
    rpuser1                                    /home/rpuser1
    ~GPO~rpuser1                               /home/GPO/rpuser1
```

The following command displays information about the home directory of user gpo\rpuser1 belonging to Vserver vs1 at share path /home/rpuser1.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1 -path /home/rpuser1
Vserver  : vs1
    Username : GPO/rpuser1
ShareName                                  Home Directory Path
    -----------------------------------
---------------------------------
    root                                       /home/rpuser1
    rpuser1                                    /home/rpuser1
    2 entries were displayed.
```

The following command displays information about the home directory of user gpo\rpuser1 belonging to Vserver vs1 at share $_{GPO}$rpuser1.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1 -share-name  ~GPO~rpuser1
Vserver  : vs1
    Username : GPO/rpuser1
ShareName                                  Home Directory Path
    -----------------------------------
---------------------------------
    ~GPO~rpuser1                               /home/GPO/rpuser1
```

vserver cifs home-directory show

Display home directory configurations

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

Description

The `vserver cifs home-directory show` command displays the CIFS home directory configuration 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>] - Vserver

If you specify this parameter, the command displays CIFS home directory configuration for the specified Vserver.

[-is-home-dirs-access-for-admin-enabled {true|false}] - Is Home Directory Access for Admin Enabled

If you specify this parameter, the command displays home directory configuration for CIFS servers that have the specified setting.

[-is-home-dirs-access-for-public-enabled {true|false}] - Is Home Directory Access for Public Enabled (privilege: advanced)

If you specify this parameter, the command displays home directory configuration for CIFS servers that have the specified setting.

Examples

The following example lists the CIFS home directory configuration for a Vserver on the cluster.

```
cluster1::> vserver cifs home-directory show -vserver vs1
Vserver: vs1
Is Home Directory Access for Admin Enabled: true
```

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.

Use an IPv4 address because WINS over IPv6 is not supported.

[-smb1-enabled {true|false}] - (DEPRECATED)-Enable SMB1 Protocol (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB 1.0 version of the CIFS protocol. The default value for this parameter is false.

This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

[-smb2-enabled {true|false}] - Enable all SMB2 Protocols (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB 2 version of the CIFS protocol. The default value for this parameter is true.

[-smb3-enabled {true|false}] - Enable SMB3 Protocol (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB 3 version of the CIFS protocol. The default value for this parameter is true.

[-smb31-enabled {true|false}] - Enable SMB3.1 Protocol (privilege: advanced)

This optional parameter specifies whether the CIFS server negotiates the SMB 3.1 version of the CIFS protocol. The default value for this parameter is true.

[-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 workgroup CIFS servers. Directories and files within a FlexGroup will not be shadow copied because FlexGroups do not support shadow copy.

[-copy-offload-enabled {true|false}] - Enable 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. Copy Offload has no effect on files in a FlexGroup because FlexGroups do not support Copy Offload.

[-is-copy-offload-direct-copy-enabled {true|false}] - Is Direct-copy Copy Offload Mechanism Enabled (privilege: advanced)

This optional parameter enables the direct-copy mechanism for ODX copy offload in the CIFS server. If set to false, the direct-copy mechanism is disabled. The default for this parameter is true. Copy Offload has no

effect on files in a FlexGroup because FlexGroups do not support Copy Offload. + The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. If turned off, regular copy offloading takes place.

[-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 Shadow Copy Feature (VSS) (privilege: advanced)

This optional parameter enables the Shadow Copy (VSS) feature in the CIFS server when set to true. The VSS feature is disabled when set to false. The default for this parameter is true. This parameter is not supported for workgroup CIFS servers. Directories and files within a FlexGroup will not be shadow copied because FlexGroups do not support shadow copy.

[-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.

[-is-local-auth-enabled {true|false}] - Is Local User Authentication Enabled (privilege: advanced)

This optional parameter specifies whether local user authentication is enabled for the CIFS server.

[-is-local-users-and-groups-enabled {true|false}] - Is Local Users and Groups Enabled (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}] - Is Reparse Point Support Enabled (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 SMB 2 or SMB 3 protocol.

[-is-exportpolicy-enabled {true|false}] - Is Export Policies for CIFS Enabled (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.

[-is-unix-nt-acl-enabled {true|false}] - Is NT ACLs on UNIX Security-style Volumes Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server has the NT ACLs enabled on UNIX security-style volumes. The default value for this parameter is true.

[-is-trusted-domain-enum-search-enabled {true|false}] - Is Enumeration of Trusted Domain and Search Capability Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports enumeration of bidirectional trusted domains. It also supports the search in all the bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. The default value is true. This parameter is not supported for workgroup CIFS servers.

[-client-session-timeout <integer>] - Idle Timeout Before CIFS Session Disconnect (secs)

This optional parameter specifies the amount of idle time (in seconds) before a CIFS session is disconnected. The default value for this parameter is 900 seconds.

[-is-dac-enabled {true|false}] - Is Dynamic Access Control (DAC) Enabled (privilege: advanced)

This optional parameter enables the Dynamic Access Control (DAC) feature in the CIFS server when set to true. The DAC feature is disabled when set to false. The default for this parameter is false. This parameter is not supported for workgroup CIFS servers.

[-restrict-anonymous {no-restriction|no-enumeration|no-access}] - Restrictions for Anonymous User (privilege: advanced)

This optional parameter controls the access restrictions of non-authenticated sessions and applies the restrictions for the anonymous user based on the permitted values. The default value for this parameter is no-restriction. Permitted values for this option are:

- no-restriction - This option specifies no access restriction for anonymous users (default).
- no-enumeration - This option specifies that only enumeration is restricted.
- no-access - This option specifies that access is restricted for anonymous users.

[-is-read-only-delete-enabled {enabled|disabled}] - Is Deletion of Read-Only Files Enabled

This optional parameter controls deletion of read-only files and directories. NTFS delete semantics forbid deletion of a file or directory when the read-only attribute is set. UNIX delete semantics ignore it, focusing instead on parent directory permissions, which some applications require. This option is used to select the desired behavior. By default this option is disabled, yielding NTFS behavior.

[-file-system-sector-size {512|4096 (in bytes)}] - Size of File System Sector Reported to SMB Clients (bytes) (privilege: advanced)

This optional parameter specifies the size of file system sector reported to SMB clients (in bytes). The default value for this parameter is 4096. Valid values are 512 and 4096.

[-is-fake-open-enabled {true|false}] - Is Fake Open Support Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports fake open requests. This parameter allows you to optimize the open and close requests coming from SMB 2 clients. The default value for this parameter is true.

[-is-unix-extensions-enabled {true|false}] - Is UNIX Extensions Enabled (privilege: advanced)

When set to true, this optional parameter enables the UNIX Extensions feature in the CIFS server. If set to false, the UNIX Extensions feature is disabled. The default for this parameter is false. UNIX Extensions allows POSIX/UNIX style security to be displayed through the CIFS protocol.

[-is-search-short-names-enabled {true|false}] - Is Search Short Names Support Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports searching short names. A search query with this option enabled will try to match 8.3 file names along with long file names. The default value for this parameter is false.

[-is-advanced-sparse-file-support-enabled {true|false}] - Is Advanced Sparse File Support Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports the advanced sparse file capabilities.

This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.

[-is-fsctl-file-level-trim-enabled {true|false}] - Is Fsctl File Level Trim Enabled (privilege: advanced)

This optional parameter specifies whether trim requests (FSCTL_FILE_LEVEL_TRIM) are supported on the CIFS server.

[-guest-unix-user <text>] - Map the Guest User to Valid UNIX User (privilege: advanced)

This optional parameter specifies that an unauthenticated user coming from any untrusted domain can be mapped to a specified UNIX user for the CIFS server. If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database, and this option is enabled, the CIFS server considers the user as a guest user and maps the user to the specified UNIX user. The UNIX user must be a valid user.

[-smb1-max-buffer-size <integer>] - Maximum Buffer Size Used for SMB1 Message (privilege: advanced)

This optional parameter specifies the maximum buffer size used for an SMB 1.0 message that the CIFS server can receive. If the LARGE_READ or LARGE_WRITE capability is negotiated during session setup, then 'Read' or 'Write' SMB 1.0 operations are allowed to exceed the configured 'smb1-max-buffer-size' value. This parameter does not have any effect on SMB 2 or SMB 3 buffer size. The default value for this parameter is 65535. The supported range for this parameter is 4356 through 65535.

[-max-same-user-sessions-per-connection <integer>] - Maximum Same User Sessions per TCP Connection (privilege: advanced)

This optional parameter specifies the maximum number of CIFS sessions that can be set up by the same user per TCP connection. The default value of this parameter is 2500. The maximum value of this parameter is 4294967295.

[-max-same-tree-connect-per-session <integer>] - Maximum Same Tree Connect per Session (privilege: advanced)

This optional parameter specifies the maximum number of CIFS tree connects to the same share per CIFS session. The default value of this parameter is 5000. The maximum value of this parameter is 4294967295.

[-max-opens-same-file-per-tree <integer>] - Maximum Opens on Same File per Tree (privilege: advanced)

This optional parameter specifies the maximum number of existing opens on the same file per CIFS tree. The default value of this parameter is 1000. The maximum value of this parameter is 4294967295.

[-max-watches-set-per-tree <integer>] - Maximum Watches Set per Tree (privilege: advanced)

This optional parameter specifies the maximum number of watches, also known as change notifies, that can be set per CIFS tree. Tree here refers to a share connect from a single client. The default value of this parameter is 500. The maximum value of this parameter is 4294967295.

[-is-admin-users-mapped-to-root-enabled {true|false}] - Map Administrators to UNIX User 'root' (privilege: advanced)

If this optional parameter is set to true, Windows users who are members of the "BUILTIN\Administrators" group are mapped to UNIX user 'root' unless a user who is a member of this group is explicitly mapped to a UNIX user. If a Windows user is a member of the "BUILTIN\Administrators" group and an explicit user mapping exists for that user, the explicit name mapping takes precedence. If this parameter is set to false, users that are members of the "BUILTIN\Administrators" group are not mapped to UNIX 'root'. The default value for this parameter is true.

[-is-advertise-dfs-enabled {true|false}] - (DEPRECATED)-Enable DFS Referral Advertisement (privilege: advanced)

This optional parameter specifies whether to advertise DFS referral of the CIFS protocol. The default value for this parameter is false. This option is not applicable to SMB 1.0.

This parameter is deprecated and may be removed in a future release of Data ONTAP. The functionality provided by this parameter is now controlled by the `-symlink-properties` parameter instead.

[-is-path-component-cache-enabled {true|false}] - Is Path Component Cache Enabled (privilege: advanced)

This optional parameter specifies whether the path component cache is enabled. The default value for this parameter is true.

[-win-name-for-null-user <TextNoCase>] - Map Null User to Windows User or Group (privilege: advanced)

This optional parameter specifies a valid Windows user or group name that will be added to the CIFS credentials for a NULL user Session.

[-is-hide-dotfiles-enabled {true|false}] - Is Hide Dot Files Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports hiding dot files. Directory enumeration with this option enabled hides files and directories that begin with a dot ("."). The default value for this parameter is false.

[-is-client-version-reporting-enabled {true|false}] - Is Client Version Reporting Enabled (privilege: advanced)

If this parameter is set to true, CIFS client version tracking information is collected by AutoSupport. The default value of this parameter is true.

[-is-client-dup-detection-enabled {true|false}] - Is Client Duplicate Session Detection Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports duplicate session detection. Duplicate sessions that come from the same client with VcNumber of zero with this option enabled will be closed, and is only applicable for SMB 1.0 clients. The default value for this parameter is true.

[-grant-unix-group-perms-to-others {true|false}] - Grant UNIX Group Permissions to Others (privilege: advanced)

This optional parameter specifies whether the incoming CIFS user who is not the owner of the file, can be granted the group permission. If the CIFS incoming user is not the owner of UNIX security-style file and this option is set to true, then at all times the file's "group" permissions are granted. If the CIFS incoming user is not the owner of UNIX security-style file and this option is set to false, then the normal UNIX rules are applicable to grant the permissions. The default value of this parameter is false.

[-is-multichannel-enabled {true|false}] - Is Multichannel Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports Multichannel or not. The default value for this parameter is false.

[-max-connections-per-session <integer>] - Maximum Connections Allowed Per Multichannel Session (privilege: advanced)

This optional parameter specifies the maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.

[-max-lifs-per-session <integer>] - Maximum LIFs Advertised Per Multichannel Session (privilege: advanced)

This optional parameter specifies the maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

[-is-large-mtu-enabled {true|false}] - Is Large MTU Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports the SMB 2.1 "large MTU" feature. The default value for this parameter is true.

[-is-netbios-over-tcp-enabled {true|false}] - Is NetBIOS over TCP (port 139) Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports the NetBIOS over TCP (port 139) feature. The default value for this parameter is true.

[-is-nbns-enabled {true|false}] - Is NBNS over UDP (port 137) Enabled (privilege: advanced)

This optional parameter specifies whether the CIFS server supports the NBNS protocol. The default value for this parameter is *false* .

[-widelink-as-reparse-point-versions <CIFS Dialects>,…] - Protocol Versions for Which Widelink Will Be Reported as Reparse Point (privilege: advanced)

This optional parameter specifies the CIFS protocol versions for which the widelink is reported as reparse point. The default value for this parameter is *SMB1* .

Any values entered for this parameter is replaced with the existing values.

[-max-credits <integer>] - Maximum Credits to Grant (privilege: advanced)

This optional parameter specifies the maximum number of outstanding requests on a CIFS connection. The default value for this parameter is 128.

[-is-share-enum-permission-check-enabled {true|false}] - Check Share Permission for NetShareEnumAll Request (privilege: advanced)

If this parameter is set to *true* , the NetShareEnum call will only respond with the shares the user has access to. The default value is *false* which means it will respond with all shares.

Examples

The following example modifies CIFS options for the Vserver "vs1". It changes the default UNIX user, disables read grants exec, changes WINS servers to 192.168.11.112 and changes the client session timeout to 6000.

```
cluster1::> vserver cifs options modify -vserver vs1
-default-unix-user pcuser -read-grants-exec disabled
-wins-servers 192.168.11.112 -client-session-timeout 6000
```

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 displays options for CIFS server with the specified UNIX user.

[-read-grants-exec {enabled|disabled}] - Read Grants Exec for Mode Bits

If this parameter is set to enabled, the command displays options for CIFS servers that grant execution access when granting read access using mode bits. If set to disabled, the command displays options for CIFS servers that 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.

[-smb1-enabled {true|false}] - (DEPRECATED)-Enable SMB1 Protocol (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where SMB 1.0 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 1.0 version of the CIFS protocol is not negotiated.

This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

[-smb2-enabled {true|false}] - Enable all SMB2 Protocols (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where SMB 2 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 2 version of the CIFS protocol is not negotiated.

[-smb3-enabled {true|false}] - Enable SMB3 Protocol (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where SMB 3 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 3 version of the CIFS protocol is not negotiated.

[-smb31-enabled {true|false}] - Enable SMB3.1 Protocol (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where SMB 3.1 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB

3.1 version of the CIFS protocol is not negotiated.

[-max-mpx <integer>] - Maximum Simultaneous Operations per TCP Connection (privilege: advanced)

If you specify this parameter, the command displays options for CIFS server with the specified maximum number of simultaneous operations the CIFS server 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 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.

[-is-copy-offload-direct-copy-enabled {true|false}] - Is Direct-copy Copy Offload Mechanism Enabled (privilege: advanced)

If set to true, this command displays options only for CIFS servers where the direct-copy mechanism for ODX Copy Offload is enabled. If set to false, options are displayed for CIFS servers where the direct- copy offload mechanism is disabled. + The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. If turned off, regular copy offloading takes place.

[-default-unix-group <text>] - Default UNIX Group

If you specify this parameter, the command displays options for CIFS server with the specified default UNIX group.

[-shadowcopy-enabled {true|false}] - Enable 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 set to true, the command displays options for the CIFS server where the CIFS server automatically refers clients to a data LIF local to the node which hosts the root of the requested share. If set to false, the command displays options for the CIFS server where the mechanism, to automatically refer the clients to data LIF local to the node which hosts the root of the requested share, is disabled.

[-is-local-auth-enabled {true|false}] - Is Local User Authentication Enabled (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}] - Is Local Users and Groups Enabled (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}] - Is Reparse Point Support Enabled (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}] - Is Export Policies for CIFS Enabled (privilege: advanced)

If you specify this parameter, the command only displays CIFS options for Vservers which have the specified export policy setting.

[-is-unix-nt-acl-enabled {true|false}] - Is NT ACLs on UNIX Security-style Volumes Enabled (privilege: advanced)

If this parameter is set to true, the command only displays CIFS options for Vservers that have the NT ACLs on UNIX security-style volumes enabled. If set to false, the command displays CIFS options for Vservers that have the NT ACLS on UNIX security-style volumes disabled.

[-is-trusted-domain-enum-search-enabled {true|false}] - Is Enumeration of Trusted Domain and Search Capability Enabled (privilege: advanced)

If this parameter is set to true, the command displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. If set to false, the command displays options for CIFS servers that do not support enumeration of bidirectional trusted domains.

[-client-session-timeout <integer>] - Idle Timeout Before CIFS Session Disconnect (secs)

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified client session timeout value (in seconds).

[-is-dac-enabled {true|false}] - Is Dynamic Access Control (DAC) Enabled (privilege: advanced)

If set to true, this command displays options only for CIFS servers where the Dynamic Access Control (DAC) feature is enabled. If set to false, options are displayed for CIFS servers where the Dynamic Access Control (DAC) feature is disabled.

[-restrict-anonymous {no-restriction|no-enumeration|no-access}] - Restrictions for Anonymous User (privilege: advanced)

If you specify this parameter, the command displays CIFS options only for CIFS servers that have the specified permitted value for the anonymous user. Permitted values for this option are:

- no-restriction - There is no access restriction for anonymous users.
- no-enumeration - Only enumeration is restricted.
- no-access - Access is restricted for anonymous users.

[-is-read-only-delete-enabled {enabled|disabled}] - Is Deletion of Read-Only Files Enabled

If you specify this parameter, the command displays options only for CIFS servers that have the specified is-read-only-delete-enabled setting.

[-file-system-sector-size {512|4096 (in bytes)}] - Size of File System Sector Reported to SMB Clients (bytes) (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified file system sector size (in bytes).

[-is-fake-open-enabled {true|false}] - Is Fake Open Support Enabled (privilege: advanced)

If you set this parameter to true, the command displays options for CIFS servers where fake open is enabled. If set to false, the command displays options for CIFS servers where fake open is disabled.

[-is-unix-extensions-enabled {true|false}] - Is UNIX Extensions Enabled (privilege: advanced)

If set to true, this command displays options only for CIFS servers where the UNIX Extensions feature is enabled. If set to false, options are displayed for CIFS servers where the UNIX Extensions feature is disabled. UNIX Extensions allows POSIX/UNIX style security to be displayed through the CIFS protocol.

[-is-search-short-names-enabled {true|false}] - Is Search Short Names Support Enabled (privilege: advanced)

If you set this parameter to true, the command displays options for CIFS servers where search short names is enabled. If set to false, the command displays options for CIFS servers where search short names is disabled.

[-is-advanced-sparse-file-support-enabled {true|false}] - Is Advanced Sparse File Support Enabled (privilege: advanced)

If set to true, the command displays options for CIFS servers where the advanced sparse file capabilities for CIFS are enabled. If set to false, options are displayed for CIFS servers where the advanced sparse file capabilities for CIFS are disabled.

[-is-fsctl-file-level-trim-enabled {true|false}] - Is Fsctl File Level Trim Enabled (privilege: advanced)

If set to true, the command displays options for all the CIFS servers where trim requests (FSCTL_FILE_LEVEL_TRIM) are supported. If set to false, options are displayed for all the CIFS servers where trim requests (FSCTL_FILE_LEVEL_TRIM) are not supported.

[-guest-unix-user <text>] - Map the Guest User to Valid UNIX User (privilege: advanced)

If you specify this parameter, the command displays options for CIFS server with the specified guest UNIX user.

[-smb1-max-buffer-size <integer>] - Maximum Buffer Size Used for SMB1 Message (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified maximum buffer size value.

[-max-same-user-sessions-per-connection <integer>] - Maximum Same User Sessions per TCP Connection (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum same user session per connection.

[-max-same-tree-connect-per-session <integer>] - Maximum Same Tree Connect per Session (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum same tree connects per session.

[-max-opens-same-file-per-tree <integer>] - Maximum Opens on Same File per Tree (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum opens on same file per tree.

[-max-watches-set-per-tree <integer>] - Maximum Watches Set per Tree (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum watches set per tree. Tree here refers to a share connect from a single client.

[-is-admin-users-mapped-to-root-enabled {true|false}] - Map Administrators to UNIX User 'root' (privilege: advanced)

If you set this parameter to true, the command displays options for CIFS servers where members of "BUILTIN\Adminstrators" group are mapped to UNIX user 'root'. If set to false, the command displays options for CIFS servers where members of the "BUILTIN\Adminstrators" group are not mapped to UNIX user 'root'.

[-is-advertise-dfs-enabled {true|false}] - (DEPRECATED)-Enable DFS Referral Advertisement (privilege: advanced)

If this parameter is set to true, the command displays CIFS options only for CIFS servers where DFS referral advertisement is enabled. If set to false, the command displays options for CIFS servers where DFS referral advertisement is disabled. This option is not applicable to SMB 1.0.

This parameter is deprecated and may be removed in a future release of Data ONTAP. The functionality provided by this parameter is now controlled by the `-symlink-properties` parameter instead.

[-is-path-component-cache-enabled {true|false}] - Is Path Component Cache Enabled (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where the path component cache is enabled. If set to false, the command displays options for CIFS servers where the path component cache is disabled.

[-win-name-for-null-user <TextNoCase>] - Map Null User to Windows User or Group (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured to add the specified windows user or group into CIFS credentials for null sessions.

[-is-hide-dotfiles-enabled {true|false}] - Is Hide Dot Files Enabled (privilege: advanced)

When set to true, this optional parameter enables the Hide Dot Files feature in the CIFS server. If set to false, the Hide Dot Files feature is disabled. The default value for this parameter is false.

[-is-client-version-reporting-enabled {true|false}] - Is Client Version Reporting Enabled (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where CIFS client version tracking is enabled. If set to false, the command displays options for CIFS servers where CIFS client version tracking is disabled.

[-is-client-dup-detection-enabled {true|false}] - Is Client Duplicate Session Detection Enabled (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where client duplicate session detection is enabled. If set to false, the command displays options for CIFS servers where client duplicate session detection is not enabled.

[-grant-unix-group-perms-to-others {true|false}] - Grant UNIX Group Permissions to Others (privilege: advanced)

If this parameter is set to true, the command displays CIFS options only for CIFS servers where grant unix

group permissions to others feature is enabled. If set to false, the command displays options for CIFS servers where grant unix group permissions to others feature is disabled.

[-is-multichannel-enabled {true|false}] - Is Multichannel Enabled (privilege: advanced)

If this parameter is set to true, the command displays options for CIFS servers where the multichannel is enabled. If set to false, the command displays options for CIFS servers where the multichannel is disabled.

[-max-connections-per-session <integer>] - Maximum Connections Allowed Per Multichannel Session (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum connections allowed per multichannel session.

[-max-lifs-per-session <integer>] - Maximum LIFs Advertised Per Multichannel Session (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum network interfaces advertised per multichannel session.

[-is-large-mtu-enabled {true|false}] - Is Large MTU Enabled (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured to support the SMB 2.1 "Large MTU" feature.

[-is-netbios-over-tcp-enabled {true|false}] - Is NetBIOS over TCP (port 139) Enabled (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured to support the NetBIOS over TCP (port 139) feature.

[-is-nbns-enabled {true|false}] - Is NBNS over UDP (port 137) Enabled (privilege: advanced)

If you specify this parameter, the command displays CIFS options only for CIFS servers that use the specified setting for the NBNS protocol.

[-widelink-as-reparse-point-versions <CIFS Dialects>,…] - Protocol Versions for Which Widelink Will Be Reported as Reparse Point (privilege: advanced)

If you specify this parameter, the command displays CIFS options only for the CIFS servers that matches the specified CIFS protocol versions for which widelinks are reported as reparse points. If a list is entered, entries are returned that matches all the specified versions.

[-max-credits <integer>] - Maximum Credits to Grant (privilege: advanced)

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified maximum credits.

[-is-share-enum-permission-check-enabled {true|false}] - Check Share Permission for NetShareEnumAll Request (privilege: advanced)

If this parameter is set to true, the command only displays CIFS options for Vservers that enabled share permission check for NetShareEnumAll request. If set to false, options are displayed for CIFS servers that disabled share permission check for NetShareEnumAll request.

Examples

The following example lists CIFS options for a Vserver on the cluster.

```
cluster1::> vserver cifs options show

Vserver: vs1
                            Client Session Timeout: 900
                                Default Unix Group: -
                                 Default Unix User: pcuser
                                   Guest Unix User: guestusers
                                  Read Grants Exec: disabled
                                       WINS Servers: -
```

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.

`[-kerberos-kdc-timeout <integer>]` - Timeout for Kerberos KDC Connections (Secs)

This parameter specifies the timeout for sockets on KDCs after which all KDCs are marked as unreachable. The default is 3 seconds.

`[-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`* for CIFS servers.

[-use-start-tls-for-ad-ldap {true|false}] - Use start_tls for AD LDAP Connections

This parameter specifies whether to use Start TLS over AD LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using Start TLS. Start TLS is a mechanism to provide secure communication by using the TLS/SSL protocols. If you do not specify this parameter, the default is *false* .

[-is-aes-encryption-enabled {true|false}] - Is AES-128 and AES-256 Encryption for Kerberos Enabled

This parameter specifies whether to use Kerberos AES-128 and AES-256 encryption types for authentication. When enabled and depending on negotiation with the KDC service, it is possible for authentication operations to utilize these encryption types. If you do not specify this parameter, the default is *false* .

[-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}] - LM Compatibility Level

This parameter specifies the LM compatibility level. The default is *lm-ntlm-ntlmv2-krb* (LM, NTLM, NTLMv2 and Kerberos).

[-is-smb-encryption-required {true|false}] - Require SMB Encryption for Incoming CIFS Traffic

This parameter specifies whether SMB encryption is required when accessing shares in the Vserver. When enabled and depending on negotiation during session setup, it is possible that data transfers between the client and the server are made secure by encrypting the SMB traffic. If you do not specify this parameter, the default is *false* .

[-session-security-for-ad-ldap {none|sign|seal}] - Client Session Security

This parameter specifies the level of security to be used for LDAP communications. If you do not specify this parameter, the default is *none* .

LDAP Client Session Security can be one of the following:

- none - No Signing or Sealing.
- sign - Sign LDAP traffic.
- seal - Seal and Sign LDAP traffic.

[-smb1-enabled-for-dc-connections {false|true|system-default}] - (DEPRECATED)-SMB1 Enabled for DC Connections

This parameter specifies whether SMB1 is enabled for use with connections to domain controllers. If you do not specify this parameter, the default is *system-default* .

SMB1 Enabled For DC Connections can be one of the following:

- false - SMB1 is not enabled.
- true - SMB1 is enabled.
- system-default - This sets the option to whatever is the default for the release of Data ONTAP that is running. For this release it is: SMB1 is enabled.

This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

[-smb2-enabled-for-dc-connections {false|true|system-default}] - SMB2 Enabled for DC Connections

This parameter specifies whether SMB2 is enabled for use with connections to domain controllers. If you do not specify this parameter, the default is *system-default*.

SMB2 Enabled For DC Connections can be one of the following:

- false - SMB2 is not enabled.
- true - SMB2 is enabled.
- system-default - This sets the option to whatever is the default for the release of Data ONTAP that is running. For this release it is: SMB2 is enabled.

[-referral-enabled-for-ad-ldap {true|false}] - LDAP Referral Chasing Enabled For AD LDAP Connections

This parameter specifies whether LDAP referral is enabled for AD LDAP connections. If you do not specify this parameter, the default is *false*.

[-use-ldaps-for-ad-ldap {true|false}] - Use LDAPS for Secure Active Directory LDAP Connections

This parameter specifies whether to use LDAPS over AD LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using LDAPS and port 636 will be used. LDAPS is a mechanism to provide secure communication by using the TLS/SSL protocols and port 636. If you do not specify this parameter, the default is *false*.

[-encryption-required-for-dc-connections {true|false}] - Encryption is required for DC Connection

This parameter specifies whether encryption is required for use with connections to domain controllers. If you do not specify this parameter, the default is *false*.

Encryption required For DC Connections can be one of the following:

- false - Encryption is not required.
- true - Encryption is required.

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
                                 Kerberos KDC Timeout:               3
seconds
                                   Is Signing Required:            true
                       Is Password Complexity Required:            true
                  Use start_tls For AD LDAP connection:           false
                              Is AES Encryption Enabled:           false
                                 LM Compatibility Level:             krb
                             Is SMB Encryption Required:           false
                                Client Session Security:            none
                      SMB1 Enabled For DC Connections:  system-default
                      SMB2 Enabled For DC Connections:  system-default
LDAP Referral Chasing Enabled For AD LDAP Connections: false
                     Use LDAPS for AD LDAP Connections: true
                Encryption required For DC Connections:           false
```

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.

[-kerberos-kdc-timeout <integer>] - Timeout for Kerberos KDC Connections (Secs)

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos KDC timeout.

[-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.

[-use-start-tls-for-ad-ldap {true|false}] - Use start_tls for AD LDAP Connections

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where Start TLS is used for communication with the AD LDAP Server. If set to *false* , the command displays CIFS security configuration information only for CIFS servers where Start TLS is not used for communication with the AD LDAP Server.

[-is-aes-encryption-enabled {true|false}] - Is AES-128 and AES-256 Encryption for Kerberos Enabled

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where AES-128 and AES-256 encryption types for Kerberos are enabled. If set to *false* , the command displays security configuration information for CIFS servers where AES-128 and AES-256 encryption types for Kerberos are disabled.

[-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}] - LM Compatibility Level

If this parameter is specified, the command displays information only about the security settings that match the specified LM compatibility level.

[-is-smb-encryption-required {true|false}] - Require SMB Encryption for Incoming CIFS Traffic

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where SMB encryption is required. If set to *false* , the command displays security configuration information for CIFS servers where SMB encryption is not required.

[-session-security-for-ad-ldap {none|sign|seal}] - Client Session Security

If this parameter is set to *seal* , the command displays CIFS security configuration information only for CIFS servers where both signing and sealing are required for LDAP communications. If set to *sign* , the command displays security configuration information for CIFS servers where only signing is required for LDAP communications. If set to *none* , the command displays security configuration information for CIFS servers where no security is required for LDAP communications.

[-smb1-enabled-for-dc-connections {false|true|system-default}] - (DEPRECATED)-SMB1 Enabled for DC Connections

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where SMB1 is enabled for use with connections to domain controllers. If set to *false* , the command displays security configuration information for CIFS servers where SMB1 is not enabled for use with connections to domain controllers. If set to *system-default* , the command displays security configuration information for CIFS servers where the system-default setting (SMB1 enabled) is used for connections to domain controllers.

This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

[-smb2-enabled-for-dc-connections {false|true|system-default}] - SMB2 Enabled for DC Connections

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where SMB2 is enabled for use with connections to domain controllers. If set to *false* , the command displays security configuration information for CIFS servers where SMB2 is not enabled for use with connections to domain controllers. If set to *system-default* , the command displays security configuration information for CIFS servers where the system-default setting (SMB2 enabled) is used for connections to domain controllers.

[-referral-enabled-for-ad-ldap {true|false}] - LDAP Referral Chasing Enabled For AD LDAP Connections

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where LDAP referral is enabled for AD LDAP connections. If set to *false* , the command displays security configuration information for CIFS servers where LDAP referral is not enabled for AD

LDAP connections.

[-use-ldaps-for-ad-ldap {true|false}] - Use LDAPS for Secure Active Directory LDAP Connections

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where LDAPS is used for communication with the AD LDAP Server. If set to *false* , the command displays CIFS security configuration information only for CIFS servers where LDAPS is not used for communication with the AD LDAP Server.

[-encryption-required-for-dc-connections {true|false}] - Encryption is required for DC Connection

If this parameter is set to *true* , the command displays CIFS security configuration information only for CIFS servers where encryption is required for use with connections to domain controllers. If set to *false* , the command displays security configuration information for CIFS servers where encryption is not required for use with connections to domain controllers.

Examples

The following example displays CIFS server security settings.

```
cluster1::> vserver cifs security show
Vserver: vs1
Kerberos Clock Skew:                3 minutes
                                  Kerberos Ticket Age:              8
hours
                                 Kerberos Renewal Age:              7
days
                                 Kerberos KDC Timeout:              3
seconds
                                   Is Signing Required:            true
                       Is Password Complexity Required:            true
                  Use start_tls For AD LDAP connection:           false
                              Is AES Encryption Enabled:           false
                                 LM Compatibility Level:             krb
                               Is SMB Encryption Required:           false
                                  Client Session Security:            none
                        SMB1 Enabled For DC Connections:  system-default
                        SMB2 Enabled For DC Connections:  system-default
LDAP Referral Chasing Enabled For AD LDAP Connections: false
                     Use LDAPS for AD LDAP Connections: true
                Encryption required For DC Connections:           false
```

The following example displays the Kerberos clock skew for all Vservers.

```
cluster1::> vserver cifs security show -fields kerberos-clock-skew
vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

vserver cifs session close

Close an open CIFS session

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

Description

The `vserver cifs session close` command closes the specified CIFS sessions.

Parameters

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

If you specify this parameter, the command will close all the opened CIFS sessions on the specified node.

`-vserver <vserver name>` - Vserver

If you specify this parameter, the command will close all the opened CIFS sessions on the specified CIFS-enabled Vserver.

`-session-id <integer>` - Session ID

If you specify this parameter, the command will close the open CIFS session that matches the specified session ID.

`[-connection-id <integer>]` - Connection ID

If you specify this parameter, the command will close all the opened CIFS sessions that match the specified connection ID.

`[-lif-address <IP Address>]` - Incoming Data LIF IP Address

If you specify this parameter, the command will close all the opened 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 will close all the opened CIFS sessions that are opened from the specified IP address.

`[-auth-mechanism <Authentication Mechanism>]` - Authentication Mechanism

If you specify this parameter, the command will close all the opened 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 will close all the opened 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 will close all the opened CIFS sessions that are established for the specified UNIX user.

[-protocol-version <CIFS Dialects>] - Protocol Version

If you specify this parameter, the command will close all the opened 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
- SMB3_1 - SMB 3.1

[-continuously-available <CIFS Open File Protection>] - Continuously Available

If you specify this parameter, the command will close all the opened 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.

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.

[-is-session-signed {true|false}] - Is Session Signed

If you specify this parameter, the command will close all the opened CIFS sessions that are established with the specified SMB signing option.

[-smb-encryption-status {unencrypted|encrypted|partially-encrypted}] - SMB Encryption Status

If you specify this parameter, the command will close all the opened CIFS sessions that are established over the specified SMB encryption status.

The SMB encryption status can be one of the following:

- unencrypted - The CIFS session is not encrypted.
- encrypted - The CIFS session is fully encrypted. Vserver level encryption is enabled and encryption happens for the entire session.
- partially-encrypted - The CIFS session is partially encrypted. Share level encryption is enabled and encryption is initiated when the tree-connect occurs.

Examples

The following example closes all open CIFS sessions on all the nodes with protocol-version SMB2:

```
cluster1::> cifs session close -node * -protocol-version SMB2
2 entries were acted on.
```

The following example closes all open CIFS sessions for all Vservers on node node1:

```
cluster1::> cifs session close -node node1 -vserver *
3 entries were acted on.
```

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.

| [-active-volumes]

If you specify this parameter, the command displays the list of Volumes that session has been connected.

| [-show-win-unix-creds]

If you specify this parameter along with a valid session-id, the command displays Windows and UNIX credentials along with the detailed information about matching CIFS sessions.

| [-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:

- None - Could not authenticate
- 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 <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Connected Time

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified time duration.

[-idle-time <[<integer>d][<integer>h][<integer>m][<integer>s]>] - 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
- SMB3_1 - SMB 3.1

[-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.

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.

`[-is-session-signed {true|false}]` - Is Session Signed

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified SMB signing option.

`[-user-type {local-user|domain-user|guest-user|anonymous-user}]` - User Authenticated as

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified user type. The user type can include one of the following:

- local-user - Authenticated as a local CIFS user
- domain-user - Authenticated as a domain user
- guest-user - Authenticated as a guest user
- anonymous-user - Authenticated as an anonymous or null user

`[-netbios-name <text>]` - NetBIOS Name

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified NetBIOS Name.

`[-smb-encryption-status {unencrypted|encrypted|partially-encrypted}]` - SMB Encryption Status

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified SMB encryption status.

The SMB encryption status can be one of the following:

- unencrypted - The CIFS session is not encrypted.
- encrypted - The CIFS session is fully encrypted. Vserver level encryption is enabled and encryption happens for the entire session.
- partially-encrypted - The CIFS session is partially encrypted. Share level encryption is enabled and encryption is initiated when the tree-connect occurs.

[-connection-count <integer>] - Connection Count

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of CIFS connections.

[-is-large-mtu-enabled {true|false}] - Is Large MTU Enabled

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified Large MTU option.

[-vol-names <volume name>,…] - Volumes List

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified volume names.

[-share-names <Share>,…] - Open Shares Lists

If you specify this parameter, the command displays information about CIFS sessions that are established including the specified share names.

Examples

The following example displays information about all CIFS sessions:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle        Connection
ID         ID      Workstation      Windows User         Files
Time             Count
---------- ------- ---------------- ---------------- ---------
--------------- -----------------
127834     1       172.17.193.172   CIFSQA\                  2
22s                 4
                                    Administrator
```

The following example displays information about a CIFS session with session-id 1.

```
cluster1::> vserver 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
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: ALIAS1
       SMB Encryption Status: encrypted
            Connection Count: 4
    Windows Unix Credentials: -
              Active Volumes: vol1,fg
```

vserver cifs session file close

Close an open CIFS file

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

Description

The `vserver cifs session file close` command closes the specified open CIFS file.

Parameters

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

If you specify this parameter, the command will close all the opened CIFS files on the specified node.

`-vserver <vserver name>` - Vserver

If you specify this parameter, the command will close all the opened CIFS files on the specified CIFS-enabled Vserver.

`-file-id <integer>` - File ID

If you specify this parameter, the command will close the opened CIFS file that matches the specified file ID.

[-connection-id <integer>] - Connection ID

If you specify this parameter, the command will close all the opened CIFS files connected on the specified connection ID.

[-session-id <integer>] - Session ID

If you specify this parameter, the command will close all the opened CIFS files connected on the specified session ID.

Examples

The following example closes all the opened CIFS files that are connected to the data LIFs of Vserver vs1 on the node node1:

```
cluster1::> vserver cifs session file close -node node1 -vserver vs1
5 entries were acted on.
```

The following example closes all the opened CIFS files on all the nodes with the file-id 1:

```
cluster1::> vserver cifs session file close -node * -file-id 1
2 entries were acted on.
```

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 session 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.

[-connection-count <integer>] - Connection Count

If you specify this parameter, the command displays information about CIFS files opened through a session that have the specified number of CIFS connections.

[-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.

[-flexgroup-msid <integer>] - FlexGroup MSID

If you specify this parameter, the command displays information about open CIFS files that reside on the volume within the FlexGroup with the specified MSID..

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
Connection Count: 4
File    File      Open Hosting                                  Continuously
ID      Type      Mode Volume          Share                    Available
------- --------- ---- --------------- ---------------------- ------------
7       Regular   rw   rootvs1         rootca                   Yes
Path: \win8b8.txt
```

The following example displays information about a CIFS file with file-id 7.

```
cluster1::> vserver cifs session file show -file-id 7 -instance
Node: node1
               Vserver: vs1
               File ID: 7
         Connection ID: 2192
            Session ID: 1
      Connection count: 4
             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
```

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. If the share is used by administrators to connect to other users' home directory (the option is-home-dirs-access-for-admin-enabled is set to true) , the dynamic share pattern must be preceded by a tilde (~).

`-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. This is a default initial property for all shares.
- attributecache - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.

  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 FlexGroups or workgroup CIFS servers.
- 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.
- 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.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

[-symlink-properties {enable|hide|read-only|symlinks|symlinks-and-widelinks|disable|no-strict-security}] - Symlink Properties

This optional parameter specifies how the storage system presents UNIX symbolic links (symlinks) to CIFS clients. The default value for this parameter is "symlinks". The list can include one or more of the following:

- enable (DEPRECATED*) - This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- hide (DEPRECATED*) - This property hides symlinks. DFS advertisements are generated if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- read-only (DEPRECATED*) - This property enables symlinks for read-only access.
- symlinks - This property enables local symlinks for read-write access. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- symlinks-and-widelinks – This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- disable - This property disables symlinks and wide links. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- no-strict-security - This property enables clients to follow symlinks outside share boundaries.

* The *`enable`* , *`hide`* , and *`read-only`* parameters are deprecated and may be removed in a future release of Data ONTAP.

The no_strict_security setting does not apply to wide links.

[-file-umask <Octal Integer>] - File Mode Creation Mask

This optional parameter specifies the default UNIX umask for new files created on the share.

[-dir-umask <Octal Integer>] - 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.

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.

[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] - Vscan File-Operations Profile

This optional parameter controls which operations trigger virus scans. The value can be one of the following:

- no-scan: Virus scans are never triggered for this share.
- standard: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- strict: Virus scans can be triggered by open, read, close, and rename operations.
- writes-only: Virus scans can be triggered only when a file that has been modified is closed.

[-max-connections-per-share <integer>] - Maximum Tree Connections on Share

This optional parameter specifies the maximum number of simultaneous connections on the new share. This limit is at the node level, not the Vserver or cluster level. The default for this parameter is 4294967295. The value 4294967295 indicates no limit. The allowed range for this parameter is (1 through 4294967295).

[-force-group-for-create <text>] - UNIX Group for File Create

This optional parameter specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. If "force-group" has been specified for a share, the following becomes true for the share:

- Primary GID of the CIFS users who access this share is temporarily changed to the GID of the "force-group".
- All files in this share that CIFS users create belong to the same "force-group", regardless of the primary GID of the file owner.

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, show-previous-versions
```

```
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
```

The following example creates a home directory share on a Vserver named vs1. The path to the share has a %d and %w combination.

```
cluster1::> vserver cifs share create -share-name %d%w -path %d/%w -share
-properties homedirectory -vserver vs1
```

The following example creates a home directory share on a Vserver vs1 to be used with the home directory option is-home-dirs-access-for-admin-enabled . The path to the share has a %d and %w combination.

```
cluster1::> vserver cifs share create -share-name ~%d~%w -path %d/%w
-share-properties homedirectory -vserver vs1
```

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. If this is a *`continuously-available`* share as specified by value of continuously-available on the `-share-properties` parameter, the path must not be within a FlexGroup because this property is not supported for FlexGroups.

[-symlink-properties {enable|hide|read-only|symlinks|symlinks-and-widelinks|disable|no-strict-security}] - 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 (DEPRECATED*) - This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- hide (DEPRECATED*) - This property hides symlinks. DFS advertisements are generated if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- read-only (DEPRECATED*) - This property enables symlinks for read-only access.
- symlinks - This property enables local symlinks for read-write access. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- symlinks-and-widelinks – This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- disable - This property disables symlinks and wide links. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- no-strict-security - This property enables clients to follow symlinks outside share boundaries.

The read_only setting does not apply to wide links.

* The *enable* , *hide* , and *read-only* parameters are deprecated and may be removed in a future release of Data ONTAP.

The no_strict_security setting does not apply to wide links.

[-file-umask <Octal Integer>] - File Mode Creation Mask

This optional parameter specifies the default UNIX umask for new files created on the share.

[-dir-umask <Octal Integer>] - 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.

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.

[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] - Vscan File-Operations Profile

This optional parameter controls which operations trigger virus scans. The value can be one of the following:

- no-scan: Virus scans are never triggered for this share.
- standard: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- strict: Virus scans can be triggered by open, read, close, and rename operations.
- writes-only: Virus scans can be triggered only when a file that has been modified is closed.

[-max-connections-per-share <integer>] - Maximum Tree Connections on Share

This optional parameter specifies a maximum number of simultaneous connections to the share. This limit is at the node level, not the Vserver or cluster level. The default for this parameter is 4294967295. The value 4294967295 indicates no limit. The allowed range for this parameter is (1 through 4294967295).

[-force-group-for-create <text>] - UNIX Group for File Create

This optional parameter specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. You can disable this option by passing a null string "".

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::> vserver cifs share modify -vserver vs1 -share-name DOCUMENTS
-share-properties branchcache,changenotify,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::> vserver cifs share modify -vserver vs1 -share-name DOCUMENTS
-share-properties changenotify,oplocks -offline-files documents
```

```
The following example modifies a CIFS share named DOCUMENTS on a Vserver
named vs1. The optional parameter "force-group-for-create" can be disabled
by passing the null string as parameter to "force-group-for-create"
option.
```

```
cluster1::> cifs share modify -vserver vs1 -share-name DOCUMENTS -force
-group-for-create ""
```

The following example modifies the symlink property of all the shares on all the Vserver to "enable".

```
cluster1::> vserver cifs share modify -vserver * -share-name * -symlink
-properties enable
```

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|symlinks|symlinks-and-widelinks|disable|no-strict-security}] - 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 Integer>] - 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 Integer>] - 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.

[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] - Vscan File-Operations Profile

If you specify this parameter, the command displays information only about the CIFS shares that have the specified Vscan fileop profile.

[-max-connections-per-share <integer>] - Maximum Tree Connections on Share

If you specify this parameter, the command displays information only about the CIFS shares that have the specified maximum connections per share configured.

[-force-group-for-create <text>] - UNIX Group for File Create

This optional parameter displays information about the CIFS shares that have the specified "force-group" parameter configured.

Examples

The following example displays information about all CIFS shares:

```
cluster1::> vserver cifs share show
Vserver        Share         Path               Properties Comment  ACL
-------------- ------------- ------------------ ---------- -------
-----------
vs1            ROOTSHARE     /                  oplocks    Share    CNC \
                                                 browsable  mapped
Everyone /
                                                 changenoti to top   Full
                                                 fy         of       Control
                                                            Vserver
                                                            global
                                                            namespac
                                                            e
vs1            admin$        /                  browsable  -        -
vs1            c$            /                  oplocks    -
BUILTIN\Admi
                                                 browsable
nistrators /
                                                 changenoti          Full
                                                 fy                  Control
vs1            ipc$          /                  browsable  -        -
4 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
      Vscan File-Operations Profile: standard
```

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.

`[-user-group-type {windows|unix-user|unix-group}]` - User or Group Type

This parameter specifies the type of the user or group to add to the CIFS share's access control list. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

`-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 windows 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 -user-group-type windows -permission Full_Control
```

The following example adds the unix-user "pcuser" and unix-group "daemon" with "read" permission to the access control list of the share "vol3".

```
vs1::> vserver cifs share access-control create -share vol3 -user-or-group
pcuser -user-group-type unix-user -permission read
        vs1::> vserver cifs share access-control create -share vol3 -user
-or-group daemon -user-group-type unix-group -permission read
```

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.

`[-user-group-type {windows|unix-user|unix-group}]` - User or Group Type

This parameter specifies the type of the user or group to delete from the CIFS share's access control list. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

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.

`[-user-group-type {windows|unix-user|unix-group}]` - User or Group Type

This parameter specifies the type of the user or group to modify. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

`[-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 windows group "Everyone" to "Full_Control".

```
vs1::*> vserver cifs share access-control modify -share vol3 -user-or
-group Everyone -user-group-type windows -permission Full_Control
```

The following example modifies the access control list for a share named "vol3". It changes the permission for the unix-user "pcuser" and unix-group "daemon" to "change".

```
vs1::> vserver cifs share access-control modify -share vol3 -user-or-group
pcuser -user-group-type unix-user -permission change
        vs1::> vserver cifs share access-control modify -share vol3 -user
-or-group daemon -user-group-type unix-group -permission change
```

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.

[-user-group-type {windows|unix-user|unix-group}] - User or Group Type

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified user-group-type. The user-group-type can be one of the following:

- windows
- unix-user
- unix-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.

[-access-mask <Hex Integer>] - Access mask

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified access rights.

Examples

The following example displays all the ACLs for shares in Vserver vs1.

```
vs1::> vserver cifs share access-control show
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            vol3        CIFSQA\administrator        windows     Read
vs1            vol3        Everyone                    windows
Full_Control
vs1            vol3        pcuser                      unix-user   Read
vs1            vol3        daemon                      unix-group  Read
```

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 ChangeNotify requests. This is a default initial property for all shares.
- attributecache - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.

  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 FlexGroups or workgroup CIFS servers.
- 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.
- 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.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

The oplock, browsable, changenotify and show-previous-versions 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".

```
cluster1::> 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 ChangeNotify requests. This is a default initial property for all shares.

- attributecache - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.

  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 FlexGroups or workgroup CIFS servers.
- 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.
- 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.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

Examples

The following example removes "showsnapshot" and "changenotify" properties to a share named "sh1".

```
cluster1::> 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 over SMB 1.0.

  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 attribute is not supported for FlexGroups and workgroup CIFS servers.
- 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.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

Examples

The following example displays share properties for shares in Vserver vs1.

```
cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              abc              oplocks
                                  browsable
                                  changenotify
                                  show-previous-versions
vs1              admin$           browsable
vs1              ipc$             browsable
vs1              sh1              oplocks
                                  browsable
                                  changenotify
                                  show-previous-versions
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. This command is not supported for workgroup CIFS servers.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Vserver name.

`-domain <CIFS domain>` - Domain (privilege: advanced)

The domain name of accountname.

`-accountname <CIFS account>` - User (privilege: advanced)

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 (privilege: advanced)

Vserver name.

`-domain <CIFS domain>` - Domain (privilege: advanced)

The domain name of accountname.

`-accountname <CIFS account>` - User (privilege: advanced)

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 (privilege: advanced)

If you specify this parameter, the command displays superuser information of only the specified Vservers.

[-domain <CIFS domain>] - Domain (privilege: advanced)

If you specify this parameter, the command displays superuser information of only for accounts that are in the specified domain.

[-accountname <CIFS account>] - User (privilege: advanced)

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 (privilege: advanced)

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, a free link (obsolete), or wide link. A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. 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.

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.

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, a free link (obsolete), or wide link. A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The default setting is `local` . The free link option is obsolete.

`[-home-directory {true|false}]` - Home Directory

This parameter specifies whether the target share is a home directory. The default value is false.

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 wide link.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /example/
-share-name EXAMPLE_SHARE
-cifs-path "/mycompany/example/" -cifs-server CIFSSERVER1 -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.

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.

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. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The default setting is `local` . The free link option is obsolete.

[-home-directory {true|false}] - Home Directory

This parameter specifies whether the new target share is a home directory.

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 wide link.

```
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, free, or wide link. (A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The free link option is deprecated and may be removed in a future release of Data ONTAP.)

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::> vserver 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 wide links:

```
cluster1::> vserver 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 remove-stale-records

Delete the Stale CIFS local users-and-groups records for the specified vserver

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

Description

The `vserver cifs users-and-groups remove-stale-records` command removes Stale local users and groups entries associated with old CIFS server.

Parameters

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

The command deletes Stale local users and groups entries associated with the specified Vserver.

Examples

The following example displays the syntax of the command.

```
cluster1::*> vserver cifs users-and-groups remove-stale-records -vserver
vs1
```

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 (privilege: advanced)

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 (privilege: advanced)

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 (privilege: advanced) }

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_grp1
               BUILTIN\Users                 AD_DOMAIN\Domain Users
                                             AD_DOMAIN\dom_usr1
               CIFS_SERVER\g1                CIFS_SERVER\u1
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\u1                  CIFS_SERVER\g1
2 entries were displayed.

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\u1

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\u1" associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\u1 -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\u1 -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\u1                  CIFS_SERVER\g1
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\u1               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 config-replication commands

vserver config-replication pause

Temporarily pause Vserver configuration replication

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

Description

Vserver domain locking functionality locks the Vserver while Vserver DM is recording a configuration baseline. This command aborts the ongoing baseline generation activity, unlocks the Vserver and temporarily pauses configuration replication for the Vserver. Command confirmations have to be enabled to execute this command. The time at which replication resumes is displayed after successful completion of the command. Configuration changes made after executing this command are not replicated to the partner cluster. If a disaster occurs during this time, the configuration changes made are lost. Replication can be manually resumed by executing the vserver config-replication resume command.

Parameters

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

== Examples

```
cluster::> vserver config-replication pause -vserver vs1
Vserver configuration replication will be paused, then automatically
resumed after five minutes.
        Manually resume configuration replication by running the "vserver
config-replication resume -vserver vs1" command.
        Do you want to continue ? {y|n}: y
Vserver configuration replication is paused and will be resumed at:
5/24/2014 06:11:23
```

Related Links

- vserver config-replication resume

vserver config-replication resume

Resume Vserver configuration replication

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

Description

This command resumes configuration replication of the Vserver which was temporarily paused by using the vserver config-replication pause command. Successful completion of the command ensures that configuration replication has been resumed for the Vserver.

Parameters

`-vserver <vserver name>` - Vserver name (privilege: advanced)

== Examples

```
cluster::> vserver config-replication resume -vserver vs1
```

Related Links

- vserver config-replication pause

vserver config-replication show

Display Vserver configuration replication resume time

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

Description

The `vserver config-replication show` command displays the time at which the configuration replication resumes 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>] - Vserver (privilege: advanced)

If you specify this parameter, the command displays resume time for the specified Vserver.

[-resume-time <MM/DD/YYYY HH:MM:SS>] - Replication resume time (privilege: advanced)

If you specify this parameter, the command displays Vservers whose configuration replications are resumed at the specified resume time.

Examples

```
cluster::> vserver config-replication show
                                    Replication
                      Vserver       Resume Time
                      -----------   -------------------
                      vs1           12/9/2014 03:18:48
```

vserver export-policy commands

vserver export-policy check-access

Given a Volume And/or a Qtree, Check to See If the Client Is Allowed Access

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

Description

The `vserver export-policy check-access` command checks whether a specific client is allowed access to a specific export path. This enables you to test export policies to ensure they work as intended and to troubleshoot client access issues.

The command takes the volume name (and optionally the qtree name) as input and computes the export path for the volume/qtree. It evaluates the export policy rules that apply for each path component and displays the policy name, policy owner, policy rule index and access rights for that path component. If no export policy rule matches the specified client IP address access is denied and the policy rule index will be set to 0. The output gives a clear view on how the export policy rules are evaluated and helps narrow down the policy and (where applicable) the specific rule in the policy that grants or denies access.

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 parameter specifies the name of the Vserver in which the export policy resides.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume that you want to check export access for. To check export access for a qtree use the -qtree parameter. The -qtree parameter is optional. If you specify the -qtree parameter, you must provide the name of the volume containing the qtree. If you do not specify the -qtree parameter, export access will be checked only for the volume.

-client-ip <IP Address> - Client IP Address

This parameter specifies the IP address of the client that you want to check export access for.

-authentication-method <authentication method> - Authentication Method

This parameter specifies the authentication method of the client that is attempting access. Possible values include the following:

- *sys* - The authentication method used by the client is AUTH_SYS.
- *krb5* - The authentication method used by the client is Kerberos v5.
- *krb5i* - The authentication method used by the client is Kerberos v5 with integrity service.
- *krb5p* - The authentication method used by the client is Kerberos v5 with privacy service.
- *ntlm* - The authentication method used by the client is CIFS NTLM.
- *none* - The authentication method used by the client is not explicitly listed in the list of values in the rorule.

-protocol <Client Access Protocol> - Protocol

This parameter specifies the protocol that the client is using when attempting to access the exported path. Possible values include the following:

- *nfs3* - The NFSv3 protocol
- *nfs4* - The NFSv4 protocol
- *cifs* - The CIFS protocol

-access-type {read|read-write} - Access Rights to Check for

This parameter specifies the type of access you want to check for. Possible values are read for read-only access and read-write for read-write access.

[-qtree <qtree name>] - Name of the Qtree

This optional parameter specifies the qtree in the volume that is part of the exported path. If you specify this parameter, you must also provide the name of the volume the qtree belongs to.

[-path <text>] - Path

Selects the entries in the output that match the specified path value. This field describes the junction-path path component encountered when evaluating the export policies starting from the root ('/') of the Vserver.

[-policy <text>] - Export Policy

Selects the entries in the output that match the specified policy value. This field describes the export policy that is in effect for the path encountered so far when evaluating the export policies starting from the root ('/') of the Vserver.

[-policy-owner <text>] - Export Policy Owner

Selects the entries in the output that match the specified policy owner value. This field describes the owner of the export policy that is in effect for the path encountered so far when evaluating the export policies starting from the root ('/') of the vserver. The owner of the export policy could be a volume or a qtree.

[-policy-owner-type {volume|qtree}] - Type of Export Policy Owner

Selects the entries in the output that match the specified type of the owner of an export policy. Possible values include the following:

- *volume* - The owner of the export policy is a volume
- *qtree* - The owner of the export policy is a qtree

[-rule-index <integer>] - Export Policy Rule Index

Selects the entries in the output that match the specified export policy rule index. This field describes the rule index of the rule in the export policy that grants or denies access. If the value of the rule index is 0 it implies none of the client match strings provided in the rules of the export policy matched the specified IP address of the client.

[-access {read|read-write}] - Access Rights

Selects the entries in the output that match the specified access value. This field describes the access rights to the path. Possible values include the following:

- *read* - Read access is granted
- *read-write* - Read-write access is granted
- *denied* - Requested access is denied

[-partial-rule-match {true|false}] - Did a Subset of the Rules Match?

Selects the entries in the output that match if a partially matched subset of rules in the export policy were used to grant access to the client.

[-clientmatch <text>] - Client Match Spec

Selects the entries in the output that match the specified clientmatch string. The clientmatch string denotes the string that resulted in a rule match for the specified client IP address.

Examples

The following examples of the `vserver export-policy check-access` command display various possible results for client export access checks.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
```

```
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read
                                        Policy    Policy       Rule
Path                          Policy    Owner     Owner Type  Index
Access
----------------------------- ---------- --------- ---------- ------
----------
/                             default    vs1_root  volume          1 read
/dir1                         default    vs1_root  volume          1 read
/dir1/dir2                    default    vs1_root  volume          1 read
/dir1/dir2/flex1              data       flex_vol  volume         10 read
4 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read-write
                                        Policy    Policy       Rule
Path                          Policy    Owner     Owner Type  Index
Access
----------------------------- ---------- --------- ---------- ------
----------
/                             default    vs1_root  volume          1 read
/dir1                         default    vs1_root  volume          1 read
/dir1/dir2                    default    vs1_root  volume          1 read
/dir1/dir2/flex1              data       flex_vol  volume         10 read-
write
4 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read-write -qtree qt1
                                        Policy    Policy       Rule
Path                          Policy    Owner     Owner Type  Index
Access
----------------------------- ---------- --------- ---------- ------
----------
/                             default    vs1_root  volume          1 read
/dir1                         default    vs1_root  volume          1 read
/dir1/dir2                    default    vs1_root  volume          1 read
/dir1/dir2/flex1              data       flex_vol  volume         10 read
/dir1/dir2/flex1/qt1          primarynames
                                        qt1       qtree           0
denied
5 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
```

```
10.22.32.42 -volume flex_vol -authentication-method ntlm -protocol cifs
-access-type read-write -qtree qt1
                                        Policy    Policy       Rule
Path                          Policy    Owner     Owner Type  Index
Access
----------------------------- --------- --------- ---------- ------
----------
/                             default   vs1_root  volume          1 read
/dir1                         default   vs1_root  volume          1 read
/dir1/dir2                    default   vs1_root  volume          1 read
/dir1/dir2/flex1              data      flex_vol  volume         10 read
/dir1/dir2/flex1/qt1          primarynames
                                        qt1       qtree           2
denied
5 entries were displayed.
```

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 <export policy name>` - 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 <export policy name>` - 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 <export policy name>` - 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
```

Related Links

- 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 <export policy name> - 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 <export policy name> - Policy Name

This parameter specifies the export policy that you want to rename.

-newpolicyname <export policy name> - 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 <export policy name>] - 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 access-cache flush

Flush an entry from the access cache

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

Description

The `vserver export-policy access-cache flush` command can be used to remove all entries in the access cache that belong to the specified export policy. The command can also be used to remove the access cache entry for a specific IP address belonging to an export policy. You must provide the name of the node that

hosts the access cache and the name of the Vserver that owns the export policy. This command differs from the vserver export-policy cache flush command. The vserver export-policy cache flush command allows you to flush all access cache entries across all export policies in a Vserver. In contrast the `vserver export-policy access-cache flush` command gives you the granularity to flush a specific access cache entry or the granularity to flush all access cache entries for a specific export policy.

This command is useful to clear out a negative access cache entry. A negative cache entry is one where a client IP address experiences an access denied error due to stale export policy rule information present in the cache entry. Data ONTAP maintains several caches in the kernel and userspace to speed access to exports. A negative cache entry can get created in the access cache if a client tries to access an export path before the export rules or the name server settings or the caches in management gateway have been updated to grant access to that client. The negative cache entry will remain in the access cache until the TTL for the entry expires and the entry is refreshed. You can use the `export-policy access-cache config show ` command to find out the refresh intervals and timeouts for the access cache. If you know that the caches in userspace have the latest information for the client and don’t want to wait until the TTL for the access cache entry expires then you can use this command to remove the access cache entry in the kernel and force the cache entry to get re-populated with the latest information that will allow the client to access the export path.

You can use the `vserver export-policy access-cache entry show` and `vserver export-policy access-cache entry show-rules` commands to examine the contents of an entry in the access cache before removing it using the flush command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to flush the access cache entry.

`-node <nodename>` - Node

This parameter specifies the node on which you want to flush the access cache entry.

`-policy <text>` - Export Policy Name

This parameter specifies the name of the export policy that is effective for the exported path that the client is trying to access.

`[-address <IP Address>]` - IP Address

This parameter is optional. It specifies the IP address of the client whose access cache entry you want to remove. If this parameter is not specified all access cache entries belonging to the specified export policy will be removed.

Examples

The following example flushes the access cache entry for client IP address '1.2.3.4' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1':

```
cluster1::*> vserver export-policy access-cache flush -vserver vs1 -node
vsim1 -policy testpol -address 1.2.3.4
Successfully removed access cache entry for IP address "1.2.3.4" belonging
to export policy "testpol" in Vserver "vs1" on node "vsim1".

cluster1::*> vserver export-policy access-cache flush -vserver vs1 -node
vsim1 -policy testpol

Warning: This command removes all access cache entries for export policy
"testpol" in Vserver "vs1" on node "vsim1". Do you want to continue?
{y|n}: y

Successfully removed 1 access cache entry for export policy "testpol" in
Vserver "vs1" on node "vsim1".
```

Related Links

- vserver export-policy cache flush

vserver export-policy access-cache show-rules

Display information about the export policy rules in the access cache entry

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

Description

The `vserver export-policy access-cache show-rules` command is used in conjunction with the vserver export-policy access-cache show command. The vserver export-policy access-cache show command displays the state and contents of an access cache entry on the specified node for a particular client IP address belonging to an export policy in a Vserver. The command lists the rule indexes of the export policy rules that matched. If you are interested in finding out the security settings for each policy rule that matched then you can use the ` vserver export-policy access-cache show-rules` command. You can use the -instance switch to get a more detailed listing. Do note that the security settings of the rules cached in the access cache entry match the security settings of the rules that can be obtained by running the vserver export-policy rule show command with the corresponding rule index.

If the client IP address is not cached in access cache then the command will display an error message stating that the entry does not exist.

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> - Node

This parameter specifies the node on which you want to examine the export policy rule details in the access cache entry.

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to see the policy rule details in the access cache entry.

-policy <export policy name> - Policy Name

This parameter specifies the name of the export policy that is in effect on the export path that the client is trying to access.

-address <IP Address> - IP Address

This parameter specifies the IP address of the client whose access cache entry you want to examine in greater detail.

[-ruleindex <integer>] - Entry Policy Rule Index

This optional parameter specifies the index number of the export rule of a specific policy.

[-protocol <Client Access Protocol>,…] - Access Protocol

This optional parameter specifies the list access protocols of export rules.

[-rorule <authentication method>,…] - RO Access Rule

This parameter specifies the security type for read-only access to volumes that use the export rule.

[-rwrule <authentication method>,…] - RW Access Rule

This parameter specifies the security type for read-write access to volumes that use the export rule.

[-superuser <authentication method>,…] - Superuser Security Types

This parameter specifies a security type for superuser access to files.

[-anon-uid <integer>] - Anonymous User ID

This parameter specifies an anonymous user ID that the user credentials are mapped to.

[-anon-gid <integer>] - Anonymous User Primary GID

This parameter specifies an anonymous User Primary GID.

[-anon-gid-list <integer>,…] - Anonymous User GID List

This parameter specifies an anonymous User Primary GID list.

[-protocol-flags {allow-suid|allow-dev}] - Protocol Flags

This parameter specifies protocol flags such as allow-suid and allow-dev.

[-ntfs-unix-security-ops {ignore|fail}] - NTFS Unix Security Options

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (fail) or allowed (ignore).

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode

This parameter specifies a change ownership mode.

[-clientmatch <text>] - Client Match String

This parameter specifies the client or clients to which the export rule applies.

[-anonuser <text>] - Anonymous Username or ID

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to.

Examples

The following example shows the contents of the access cache entry for client IP address '1.2.3.4' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1'. This entry has two export policy rules with rule indexes 1 and 2 that matched and are cached in the entry. To examine what the rule settings are in each of these rules we can use the show-rules variant of the command.

```
cluster1::*>vserver export-policy access-cache show -vserver vs1 -node
vsim1 -policy testpol -address 1.2.3.4
Node: vsim1
                            Vserver: vs1
                        Policy Name: testpol
                         IP Address: 1.2.3.4
           Access Cache Entry Flags: -
                        Result Code: 0
                   Failure Type Code: 0
     Number of Matched Policy Rules: 2
List of Matched Policy Rule Indexes: 1, 2
                       Age of Entry: 5s

cluster1::*>vserver export-policy access-cache show-rules -vserver vs1
-node vsim1 -policy testpol -address 1.2.3.4
                                     Rule  Access   RO    RW    Super Anon
Node       Address         Policy    Index Protocol Rule  Rule  User  User
---------- --------------- --------- ----- -------- ----  ----  ----- -----
vsim1      1.2.3.4         testpol   1     any      any   any   none  65534
vsim1      1.2.3.4         testpol   2     nfs3     never never sys   123
2 entries were displayed.

cluster1::*>vserver export-policy access-cache show-rules -vserver vs1
-node vsim1 -policy testpol -address 1.2.3.4 -instance
Vserver: vs1
                      Node: vsim1
               Policy Name: testpol
                IP Address: 1.2.3.4
          Export Policy ID: 12884901890
   Entry Policy Rule Index: 1
           Access Protocol: any
            RO Access Rule: any
```

```
            RW Access Rule: any
  Superuser Security Types: none
         Anonymous User ID: 65534
            Protocol Flags: allow-suid, allow-dev
NTFS Unix Security Options: fail
     Change Ownership Mode: restricted
Vserver: vs1
                      Node: vsim1
               Policy Name: testpol
                IP Address: 1.2.3.4
             Export Policy: testpol
          Export Policy ID: 12884901890
   Entry Policy Rule Index: 2
           Access Protocol: nfs3
            RO Access Rule: never
            RW Access Rule: never
  Superuser Security Types: sys
         Anonymous User ID: 123
            Protocol Flags: allow-suid
NTFS Unix Security Options: ignore
     Change Ownership Mode: restricted
2 entries were displayed.

cluster1::*> vserver export-policy rule show -vserver vs1 -policyname
testpol -ruleindex 1
                                    Vserver: vs1
                                Policy Name: testpol
                                 Rule Index: 1
                             Access Protocol: any
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                              RO Access Rule: any
                              RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: none
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true

cluster1::*> vserver export-policy rule show -vserver vs1 -policyname
testpol -ruleindex 2
                                    Vserver: vs1
                                Policy Name: testpol
                                 Rule Index: 2
                             Access Protocol: nfs3
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                              RO Access Rule: never
                              RW Access Rule: never
```

```
User ID To Which Anonymous Users Are Mapped: testu1
                    Superuser Security Types: sys
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: false
```

Related Links

- vserver export-policy access-cache show
- vserver export-policy rule show

vserver export-policy access-cache show

Display information about the access cache entry

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

Description

The `vserver export-policy access-cache show` command can be used to display the contents of an access cache entry of the specified node for a particular client IP address belonging to an export policy in a Vserver.

The command will display information such as the flags of the access cache entry, the age of the entry, any errors that were encountered when looking up the export policy rules from the management gateway, and the number of policy rules from the export policy that matched the specified client IP address. If an error is encountered when looking up the export policy rules from the management gateway process, the first rule index in the export policy that encountered the error is displayed. The client match string or the anon string in the rule that caused the rule evaluation to fail is also displayed. A more detailed view of the output of this command is available if you specify the -instance switch to the command.

The command output lists the rule indexes of the policy rules that matched. If you are interested in finding out the security settings for each policy rule that matched then you can use the vserver export-policy access-cache show-rules command.

If the client IP address is not cached in the access cache then the command will display an error message stating that the entry does not exist.

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> - Node

This parameter specifies the node on which you want to examine the access cache entry.

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to see the access cache entry.

-policy <export policy name> - Policy Name

This parameter specifies the name of the export policy that is in effect on the export path that the client is trying to access.

-address <IP Address> - IP Address

This parameter specifies the IP address of the client whose access cache entry you want to examine.

[-flags {pending|refreshing|is-abandoned|is-queued-for-update|is-updating|has-usable-data}] - Access Cache Entry Flags

Selects the access cache entries that match the specified flags value. The flags describe the internal state of the access cache entry. The access cache entry could be in 'pending' state. This denotes the initial state of the access cache entry when a client first tries to access the exported mount point and the rules in the export policy are being matched against the IP address of the client. The 'refreshing' state denotes that the access cache entry is being refreshed. The 'abandoned' state denotes that the access cache entry has been cleared as a result of a cache flush operation. If the access cache entry has been successfully evaluated this field will not be set to any value.

[-result <integer>] - Result Code

Selects the access cache entries that match the specified result value. This field describes the error code of the error encountered when matching the IP address of the client against the rules specified in the export policy. If all rules were evaluated successfully this field will be set to 0.

[-first-unresolved-index <integer>] - First Unresolved Rule Index

Selects the access cache entries that match the specified unresolved rule index value. This field describes the rule index of the first rule in the export policy that could not be evaluated successfully when matching the IP address of the client against the rules specified in the export policy. If all rules were evaluated successfully this field will not be set to any value.

[-unresolved-clientmatch <text>] - Unresolved Clientmatch

Selects the access cache entries that match the specified unresolved client match value. This field describes the client match string that caused the rule evaluation to fail at the displayed rule index. Client match strings that denote a netgroup, hostname or a domain name can fail in evaluation if there are problems in contacting the name servers configured to serve them. If all rules were evaluated successfully this field will not be set to any value.

[-num-rules <integer>] - Number of Matched Policy Rules

Selects the access cache entries that match the specified number of matched export rules. This field describes the number of rules in the export policy that were matched successfully against the IP address of the client. If the number of matched rules is 0 and the 'result' field is also 0 then the client will experience an access denied error during mount. If the number of matched rules is non-zero and the 'result' field is 0 then access is granted or denied based on the ro, rw, superuser and other security settings in the matched rules. If the number of matched rules is 0 and the 'result' field has a non-zero value in it the client will experience a hang until the error that caused the rule evaluation to fail is resolved. If the number of matched rules is non-zero and the 'result' field has a non-zero value then this represents a situation where an error was encountered that stopped the match of rules in the export policy against the IP address of the client. The rules that have matched so far are used to make access decisions. (Note that the match of rules follows an ordering precedence determined by the rule index). Access may be granted if the security settings in the rules that have matched so far allow access. The security settings in the partial subset of matched rules are never used to deny access because they represent an incomplete set of matched export rules. Instead the

client will experience a hang until the error that caused the rule evaluation to fail is resolved.

[-ruleindex-list <integer>,…] - List of Matched Policy Rule Indexes

Selects the access cache entries that match the specified list of matched rule indexes. This field describes a comma separated list of the indexes of the rules in the export policy that matched the IP address of the client. If no rules match the IP address of the client or an error was encountered in the client match process then this field will not be set to any value.

[-age <[<integer>h][<integer>m][<integer>s]>] - Age of Entry

Selects the access cache entries that match the specified age of the entry. This field describes the age of the access cache entry.

[-polarity {positive|negative|init}] - Access Cache Entry Polarity

Selects the access cache entries that match the specified polarity of the entry. The polarity of an access cache entry can be positive or negative. A positive polarity denotes that access is granted to the client IP address. A negative polarity denotes that access is denied to the client IP address.

[-duration-since-last-use <[<integer>h][<integer>m][<integer>s]>] - Time Elapsed since Last Use for Access Check

Selects the access cache entries that match the specified time duration since the entry was last used for access determination.

[-duration-since-last-update-attempt <[<integer>h][<integer>m][<integer>s]>] - Time Elapsed since Last Update Attempt

Selects the access cache entries that match the specified time duration since the access cache entry was last updated.

[-last-update-attempt-result <integer>] - Result of Last Update Attempt

Selects the access cache entries that match the specified result obtained when the access cache entry was last updated.

[-clientmatch-list <text>,…] - List of Client Match Strings

Selects the access cache entries that match the specified list of clientmatch strings that matched the specified client IP address.

Examples

The following example shows the contents of the access cache entry for client IP address '10.22.33.32' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1':

```
cluster1::*> vserver export-policy access-cache show -vserver vs1 -policy
testpol -node vsim1 -address 10.22.33.32
Node: vsim1
                                        Vserver: vs1
                                    Policy Name: testpol
                                     IP Address: 10.22.33.32
                           Access Cache Entry Flags: has-usable-data
                                    Result Code: 0
                      First Unresolved Rule Index: -
                           Unresolved Clientmatch: -
                  Number of Matched Policy Rules: 1
              List of Matched Policy Rule Indexes: 20
                                  Age of Entry: 77s
                      Access Cache Entry Polarity: positive
          Time Elapsed since Last Update Attempt: 8s
    Time Elapsed since Last Use for Access Check: 3s
                   Result of Last Update Attempt: 7208
                    List of Client Match Strings: 0.0.0.0/0
```

Related Links

- vserver export-policy access-cache show-rules

vserver export-policy access-cache config modify-all-vservers

Modify exports access cache configuration for all Vservers

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

Description

The `vserver export-policy access-cache config modify-all-vservers` command modifies access cache timeout values for all Vservers. Modifying these values from any node updates the values on all the nodes in the cluster. The modified values persist across reboots.

> This command is not supported in a cluster with effective cluster version of Data ONTAP 9.0.0 or later. The access cache settings are modified on a per-Vserver basis starting Data ONTAP 9.0.0. See the vserver export-policy access-cache config modify command.

Parameters

`[-ttl-positive <integer>]` - TTL For Positive Entries (Secs)

This parameter specifies the duration after which positive access cache entries will be refreshed when the client accesses.

`[-ttl-negative <integer>]` - TTL For Negative Entries (Secs)

This parameter specifies the duration after which negative access cache entries will be refreshed when the client accesses.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

This parameter specifies the time period after which Data ONTAP deletes unused entries in the access cache.

Examples

The following command sets the positive TTL value to 36000 seconds, the negative TTL value to 3600 seconds, and the harvest timeout value to 43200 seconds for all Vservers in a cluster where the effective cluster version is earlier than Data ONTAP 9.0.0.

```
cluster1::*> vserver export-policy access-cache config modify-all-vservers
-ttl-positive 36000 -ttl-negative 3600 -harvest-timeout 43200

cluster1::*> vserver export-policy access-cache config show-all-vservers
     TTL For Positive Entries (secs): 36000
     TTL For Negative Entries (secs): 3600
              Harvest Timeout (secs): 43200
```

Related Links

- vserver export-policy access-cache config modify

vserver export-policy access-cache config modify

Modify exports access cache configuration

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

Description

The `vserver export-policy access-cache config modify` command modifies access cache timeout values per Vserver. Modifying these values from any node updates the values on all the nodes in the cluster. The modified values persist across reboots.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver name for which the timeout values need to be modified.

[-ttl-positive <integer>] - TTL For Positive Entries (Secs)

This parameter specifies the duration after which positive access cache entries will be refreshed upon client access. The value is specified in seconds. The default value is 3600 seconds. Valid values range from 300 seconds to 86400 seconds.

[-ttl-negative <integer>] - TTL For Negative Entries (Secs)

This parameter specifies the duration after which negative access cache entries will be refreshed upon client access. The value is specified in seconds. The default value is 3600 seconds. Valid values range from 60 seconds to 86400 seconds.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

This parameter specifies the time period after which Data ONTAP deletes unused entries in the access cache. The value is specified in seconds. The default value is 86400 seconds. Valid values range from 60 seconds to 2592000 seconds.

Examples

The following command sets the positive TTL value to 36000 seconds, the negative TTL value to 3600 seconds, and the harvest timeout value to 43200 seconds for Vserver 'vs0':

```
cluster1::*> vserver export-policy access-cache config modify -ttl
-positive 36000 -ttl-negative 3600 -harvest-timeout 43200

cluster1::*> vserver export-policy access-cache config show -vserver vs0
Vserver: vs0
    TTL For Positive Entries (secs): 36000
    TTL For Negative Entries (secs): 3600
TTL For Entries with Failure (secs): 1
             Harvest Timeout (secs): 43200
```

vserver export-policy access-cache config show-all-vservers

Display exports access cache configuration for all Vservers

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

Description

The `vserver export-policy access-cache config show-all-vservers` command displays the timeout attributes related to the exports access cache. The access cache maintains export rules applicable to a client that is accessing the volume or qtree. Data ONTAP obtains the access cache timeout values from the node where you run the command. The command output displays the following timeout parameters and their values:

- TTL for Positive Entries: This is the TTL for positive entries in the access cache. During client access, if the TTL for the access cache entry that is allowing access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- TTL for Negative Entries: This is the TTL for negative entries in the access cache. During client access, if the TTL for the access cache entry that is denying access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- Harvest Timeout: If Data ONTAP does not use an entry that is stored in the access cache for this period of time, it deletes the entry.

This command is not supported in a cluster with effective cluster version of Data ONTAP 9.0.0 or later. The access cache settings are stored on a per-Vserver basis starting Data ONTAP 9.0.0. See the vserver export-policy access-cache config show command.

Examples

The following command displays the exports access cache timeout values for all Vservers in a cluster where the effective cluster version is earlier than Data ONTAP 9.0.0:

```
cluster1::*> vserver export-policy access-cache config show-all-vservers
     TTL For Positive Entries (secs): 36000
     TTL For Negative Entries (secs): 3600
              Harvest Timeout (secs): 43200
```

Related Links

- vserver export-policy access-cache config show

vserver export-policy access-cache config show

Display exports access cache configuration

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

Description

The `vserver export-policy access-cache config show` command displays the timeout attributes related to the exports access cache. The access cache maintains export rules applicable to a client that is accessing the volume or qtree. The command output displays the following timeout parameters and their values for each Vserver:

- TTL for Positive Entries: This is the TTL for positive entries in the access cache. During client access, if the TTL for the access cache entry that is allowing access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- TTL for Negative Entries: This is the TTL for negative entries in the access cache. During client access, if the TTL for the access cache entry that is denying access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- TTL for Entries with Failure: This is the TTL for access cache entries for which a failure was encountered while trying to get matching rules.
- Harvest Timeout: If Data ONTAP does not use an entry that is stored in the access cache for this period of time, it deletes the entry.

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 the timeout values for the specified Vserver.

[-ttl-positive <integer>] - TTL For Positive Entries (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose ttl-positive matches the provided value.

[-ttl-negative <integer>] - TTL For Negative Entries (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose ttl-negative matches the provided value.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose harvest-timeout matches the provided value.

Examples

The following command displays the exports access cache timeout values for all Vservers in the cluster:

```
cluster1::*> vserver export-policy access-cache config show
Vserver  TTL Positive  TTL Negative TTL Failure Harvest Timeout
               (secs)        (secs)      (secs)          (secs)
-------- ------------- ------------ ----------- ---------------
vs0               300            60           1            3600
vs1             36000          3600           5            3600
2 entries were displayed.
```

vserver export-policy cache flush

Flush the Export Caches

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

Description

The `vserver export-policy cache flush` command clears out the contents of the export policy caches for a Vserver. You might need to flush the caches to allow the changes to immediately take effect for your NFS clients because of:

- A change to your export policy rules.
- Modifying a host name record in a name server (i.e., local hosts or DNS).
- Modifying a PTR record in a DNS server (i.e., reverse DNS lookup).
- Modifying the entries in a netgroup in a name server (i.e., local netgroup, LDAP, or NIS).
- Recovering from a network outage that resulted in a netgroup being partially expanded.

To flush the caches, you must specify the following items:

- Vserver: either a specific Vserver or use "*" to flush all of them.

You can optionally specify the following items:

- Node: if flushing the *access* cache, you can also specify which node to flush it on.
- Cache to flush: by default all but *showmount* will be flushed.

Note that the *showmount* cache is not used to determine NFS client access and as such is only flushable explicitly.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to flush the caches.

[-node <nodename>] - Node

This parameter specifies the node on which you want to flush the *access* cache.

[-cache {all|access|host|id|name|netgroup|showmount|ip}] - Cache Name

This parameter specifies the name of the cache which you want to flush. Possible values include the following:

- *all* - All caches but *showmount* . This is the default.
- *access* - The export-policy rules access cache.
- *host* - The host name to IP cache.
- *id* - The ID to credential cache.
- *ip* - The IP to host name cache.
- *name* - The name to ID cache.
- *netgroup* - The netgroup cache.
- *showmount* - The showmount caches.

Examples

The following example flushes the access cache on a Vserver named vs0:

```
cluster1::> vserver export-policy cache flush -vserver vs0 -cache access
```

vserver export-policy config-checker show

Show the status of export policy configuration checker jobs

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

Description

The `vserver export-policy config-checker show` command displays status information about export policy configuration checker job. This command displays the following information:

- Vserver name
- Export policy name
- Export policy configuration checker job state
- Export policy rule checked count
- Export policy rule being checked rule index
- Export policy rule with issue count

This command output will only be available after running the export policy configuration checker job.

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 export policy configuration checker job state information for Vservers that match the specified value.

[-policy <export policy name>] - Policy Name

If you specify this parameter, the command displays export policy configuration checker job state information for policy that match the specified value.

[-rules-checked <integer>] - Number of Rules Checked

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rules-checked count matching.

[-rule-being-checked <integer>] - Rule Being Checked

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rule-being-checked index matching.

[-rules-with-issues <integer>] - Number of Rules with Issues

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rules-with-issues count matching.

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

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified state matching.

Examples

The following example displays an export policy configuration checker job state information for vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker show -vserver vs2 -policy
default
Job       Rules     Rule Index    Rules With
Vserver    Policy     State     Checked   Being Checked Issues
---------- ---------- --------- --------- ------------- -------------
vs2        default    Running   1         2             1
```

vserver export-policy config-checker start

Start export policy configuration checker job

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

Description

The `vserver export-policy config-checker start` command invokes background job, which will check export policy configuration and if issue found in rules then error entry is created for each affected rule in export policy configuration checker error rule list.

Export policy configuration checker only validates hostname, netgroup and anonymous user related configuration.

Parameters

`-vserver <vserver name>` - Vserver

If you specify this parameter, the export policy configuration checker job will be triggered for specified Vserver.

`[-policy <export policy name>]` - Export Policy Name

If you specify this parameter, the export policy configuration checker job will be triggered for specified policy.

Examples

The following example start a export policy configuration checker job for vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker start -vserver vs2
-policy default
          [Job 644] Job is queued: Export Policy configuration checker.
```

vserver export-policy config-checker stop

Stop export policy configuration checker job

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

Description

The `vserver export-policy config-checker stop` command stops running export policy configuration checker job.

> Export policy configuration checker stop command only works if the keys provided are same as the keys provided at the time of starting export policy configuration checker job.

Parameters

`-vserver <vserver name>` - Vserver

If you specify this parameter, the command stops export policy configuration checker job, if any export policy configuration checker job is running for the specified Vserver.

`[-policy <export policy name>]` - Export Policy Name

If you specify this parameter, the command stops export policy configuration checker job, if any export policy configuration checker job is running for the specified policy.

Examples

The following example stop an export policy configuration checker job for Vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker stop -vserver vs2 -policy
default
```

vserver export-policy config-checker rule delete

Delete error entries for rules from export policy configuration checker error rule list

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

Description

The `vserver export-policy config-checker rule delete` command deletes error rule entries from export policy configuration checker error rule list. You can delete a specific error entry rule by specifying its rule index number.

Parameters

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

This parameter specifies the node on which the export policy configuration error rule entries are stored.

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver which contains the export policy.

`-policy <export policy name>` - Policy Name

This parameter specifies the export policy from which you want to delete an error rule entry.

-rule-index <integer> - Rule Index

This parameter specifies the index number of the error rule entry that you want to delete. You can use the vserver export-policy config-checker rule show command to view a list of rules with their index numbers.

Examples

The following example deletes an error rule entry from config-checker error rule list, with the index number 1 from an export policy named default on a Vserver named vs34:

```
cluster1::>vserver export-policy config-checker rule delete -node node-
vsim3 -vserver vs34 -policy test -rule-index 1
  (vserver export-policy config-checker rule delete)
1 entry was deleted.
```

Related Links

- vserver export-policy config-checker rule show

vserver export-policy config-checker rule show

Show error entries for rules in export policy configuration checker job

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

Description

The `vserver export-policy config-checker rule show` command displays information about error related to configuration in export policy rules. If a rule has any issues the configuration checker job will log information about such errors on the node where the job runs. The command displays the following information:

- Node name
- Vserver name
- Export policy name
- Export policy rule index number
- Export policy rule error

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.

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

If you specify this parameter, the command displays detailed error information for node that matches the specified value.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays detailed error information for Vservers that match the specified value.

[-policy <export policy name>] - Policy Name

If you specify this parameter, the command displays detailed error information for policy that match the specified value.

[-rule-index <integer>] - Rule Index

If you specify this parameter, the command displays detailed error information for rule-index that match the specified value.

[-error <text>] - Error Details

If you specify this parameter, the command displays rule index information for error that match the specified value. The complete error string needs to be specified within "{}".

Examples

The following example displays information about error related to export rules:

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test
  (vserver export-policy config-checker rule show)
                         Rule
Node       Vserver      Policy    Index     Error
---------- ------------ --------- ---------
---------------------------------
node-vsim3
           vs34         test      1         DNS lookup for host "h1"
failed
           vs34         test      2         Entry not found for "UserName:
testuser", DNS lookup for host "h2" failed
2 entries were displayed.
```

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test -rule-index 1
  (vserver export-policy config-checker rule show)
Node: node-vsim3
      Vserver: vs34
  Policy Name: test
   Rule Index: 1
Error Details: DNS lookup for host "h1" failed
```

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test -error  {DNS lookup for host "h1" failed}
  (vserver export-policy config-checker rule show)
                         Rule
Node       Vserver      Policy    Index     Error
---------- ------------ --------- ---------
-----------------------------------
node-vsim3
           vs34         test      1         DNS lookup for host "h1"
failed
```

vserver export-policy netgroup check-membership

Check to see if the client is a member of the netgroup

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

Description

The `vserver export-policy netgroup check-membership` command determines if the client IP address is a member of the netgroup. Data ONTAP can determine the membership information only after it has fully loaded the netgroup into the cache. Until then, while the reverse lookup scan algorithm might find a match, both DNS round robin and DNS aliases prevent ruling out non-matches. You can use the vserver export-policy netgroup queue show command to monitor the loading of the netgroup.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver whose netgroup you want to check for client membership.

`-netgroup <text>` - Name of the Netgroup

This parameter specifies the name of the netgroup that you want to check for client membership.

`-client-ip <IP Address>` - Client Address

This parameter specifies the IP address of the client whose netgroup membership you want to check.

Examples

The following examples of the `vserver export-policy netgroup check-membership` command display various possible results for client membership checks.

```
cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
Client 172.17.16.72 is a member of netgroup "mercury" for Vserver "vs1"
with state "reverse lookup scan".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
Client 172.17.16.72 is a member of netgroup "mercury" for Vserver "vs1"
with state "cache".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.14
Client 172.17.16.14 is not a member of netgroup "mercury" for Vserver
"vs1".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 172.17.16.69
Cannot yet determine the membership of client 172.17.16.69 in netgroup
"big" for Vserver "vs1". Try again when the netgroup is loaded in the
cache.

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 172.17.16.69
Client 172.17.16.72 is a member of netgroup "big" for Vserver "vs1" with
state "cache".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 2002:c65f:e228:0:0:0:0:0
Cannot yet determine the membership of client 2002:c65f:e228:: in netgroup
"big" for Vserver "vs1". Try again when the netgroup is loaded in the
cache.
```

Related Links

- vserver export-policy netgroup queue show

vserver export-policy netgroup cache show

Show the Netgroup Cache

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

Description

The `vserver export-policy netgroup cache show` command displays the contents of the export policy netgroup cache for a Vserver. Entries shown here correspond to the caches used to evaluate client membership in a netgroup. To show the netgroup cache, you must specify the following item:

- Vserver: The name of the Vserver whose netgroup cache you want to display.

The following information is displayed per cache entry:

- Vserver name: The name of the Vserver.
- Netgroup name: The name of the netgroup.
- State of the cache entry: The state of the cache entry. There are four possible values:
- initializing: The cache entry is being populated for the first time.
- ready: Processing of the cache entry is complete and it is ready to be used.
- not-found: The netgroup could not be found.
- abandoned: The cache entry has been abandoned.
- Total number of hosts in the netgroup cache: The number of host names retrieved from the name service in mapping the netgroup to a list of hosts.
- How long it took to expand the netgroup: How long it took to expand the netgroup the last time in the queue.
- Entry is refreshing: If the entry is a complete miss or refresh.
- Next refresh time: When the next refresh is scheduled to take place.
- Netgroup by host state: Boolean state indicating if netgroup-by-host feature is used for resolving netgroup membership check.
- Number of IP addresses cached: Number of client IP addresses that are matched for the netgroup. The count includes both positive and negative results.

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 the netgroup cache information only if the Vserver name matches the specified value.

[-netgroup <text>] - Name of the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup name matches the specified value.

[-cache-state {initializing|ready|not-found|abandoned}] - State of the Cache Entry

If you specify this parameter, the command displays the netgroup cache information only if the netgroup cache state matches the specified value.

[-total-hosts <integer>] - Total Number of Hosts in the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record’s count of host names matches the specified value.

[-expansion-duration <[[<hours>:]<minutes>:]<seconds>>] - Expansion Duration

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record expansion time matches the specified value.

[-is-refreshing {true|false}] - Is Entry Refreshing?

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record refreshing state matches the specified value.

[-time-next-refresh <Date>] - Next Refresh Time

If you specify this parameter, the command displays the netgroup cache information only if the time of the next scheduled refresh matches the specified value.

[-num-ip-addrs-cache <integer>] - Number of Cached IP Addresses

If you specify this parameter, the command displays the netgroup cache information only if the number of cached IP addresses matches the specified value.

Examples

The following example displays the netgroup cache for the Vserver vs1 and the netgroup netgroup1:

```
cluster1::> vserver export-policy netgroup cache show -vserver vs1
-netgroup netgroup1
Vserver  Netgroup   State
    -------- ---------- ------------
    vs1      netgroup1  Ready
```

vserver export-policy netgroup queue show

Show the Netgroup Processing Queue

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

Description

The `vserver export-policy netgroup queue show` command displays the ongoing processing of the netgroup cache for a node. Entries shown here are not used to evaluate client membership in a netgroup. The following information is displayed per queue entry:

- Vserver name: The name of the Vserver.
- Netgroup name: The name of the netgroup.
- Age of entry in the queue: How long the entry has been in the queue.
- Queue state: The state of the entry in the queue. There are three possible values:
- running: The entry is currently being processed.
- waiting: The entry is waiting to be processed.
- retrying: The entry is waiting to be reprocessed.

```
 Note that as the `vserver export-policy netgroup queue show` command is
not atomic. Several queue entries might show up in the 'running' state.
* Number of times retried in the queue: The number of times was the
entry was taken off of the netgroup processing queue and added back on
it.
* Total number of hosts in the netgroup: The number of host names
retrieved from the name service in mapping the netgroup to a list of
hosts.
```

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 the netgroup cache information only if the Vserver name matches the specified value.

[-netgroup <text>] - Name of the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup name matches the specified value.

[-queue-state {waiting|running|retrying}] - State of Entry in the Queue

If you specify this parameter, the command displays the netgroup cache information only if the netgroup queue state matches the specified value.

[-age <[[<hours>:]<minutes>:]<seconds>>] - Age of Entry in the Queue

If you specify this parameter, the command displays the netgroup cache information only if the age of when the netgroup record was put on the netgroup processing queue matches the specified value.

[-retries-on-queue <integer>] - Number of Retries on the Queue

If you specify this parameter, the command displays the netgroup cache information only if, during a refresh, the number of times the netgroup record has been put back on the netgroup processing queue matches the specified value.

[-total-hosts <integer>] - Total Number of Hosts in the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record’s count of hosts matches the specified value.

Examples

The following example displays the netgroup queue:

```
cluster1::> vserver export-policy netgroup queue show
                                        Age on     Total
    Vserver    Netgroup   State          Queue     Hosts
    ---------- ---------- --------- --------- ---------
    testvs1    test-netgr retrying     0:0:47     12441
    testvs1    test       waiting     0:01:35         -
```

vserver export-policy rule add-clientmatches

Add list of clientmatch strings to an existing rule

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

Description

The `vserver export-policy rule add-clientmatches` command adds a list of strings to the clientmatch field of a specified export rule in a policy. This command only operates on the clientmatch field; to modify other fields in a rule use the `vserver export-policy modify` command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy containing the export rule to which you want to add additional clientmatch strings.

`-ruleindex <integer>` - Rule Index

This parameter specifies the index number of the export rule to which you want to add additional clientmatch strings. To view a list of rules with their index numbers, use the vserver export-policy rule show command.

`-clientmatches <text>` - List of Clientmatch Strings to Add

This parameter specifies list of the match strings specifying the client or clients to add to the export rule. Duplicate match strings will not be created and the list may not contain duplicates entries. Match strings from the clientmatches list are added to the clientmatch field if the match string is not identical to one of the strings already in the clientmatch field. You can specify the match string 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, 10.1.12.0/24
- 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.

Examples

The following example adds match strings "2.2.2.2" and "3.3.3.3" to the clientmatch field of the export rule with index number 3 in an export policy named default_expolicy on a Vserver named vs0.

```
cluster1::> vserver export-policy rule add-clientmatches -vserver vs0
-policyname default_expolicy -ruleindex 3 -clientmatches "2.2.2.2,3.3.3.3"
```

Related Links

- vserver export-policy rule show

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 <export policy name>` - 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 <Client Access Protocol>,…]` - 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

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* . If you enable NFSv4, you will not be able to apply the policy to which this rule belongs to a FlexGroup, as FlexGroups do not support NFSv4 protocol access.

`-clientmatch <text>` - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

This parameter specifies list of the match strings specifying the client or clients to which the export rule applies. Duplicate match strings in the same rule are not allowed. You can specify the match string 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, 10.1.12.0/24
- 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 <authentication method>,… - 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 v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- *krb5i* - 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 v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - 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 v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *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.

  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.

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 <authentication method>,… - 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 v5.
- *krb5i* - 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 v5 with integrity service.
- *krb5p* - 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 v5 with privacy service.
- *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.

  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.

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. NFS clients typically associate user ID 65534 with the user name nobody. In clustered Data ONTAP, this user ID is associated with the user pcuser. To disable access by any client with a user ID of 0, specify a value of 65535 which is associated with the user nobody.

[-superuser <authentication method>,…] - 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 v5.
- *krb5i* - 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 v5 with integrity service.

- *krb5p* - 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 v5 with privacy service.
- *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.

  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.

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 who is allowed to change the ownership mode of a file. The default setting is `restricted` . The allowed values are:

- restricted - Only root may change the ownership of the file.
- unrestricted - Non-root users may change file ownership provided the on-disk permissions allow the operation.

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 domains named example.com

or example.net. 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.

```
cluster1::> vserver export-policy rule create -vserver vs0 -policyname
read_only_expolicy -ruleindex 1
-protocol any -clientmatch ".example.com,.example.net" -rorule any -rwrule
"ntlm,krb5,sys" -anon 65534 -allow-suid false
-allow-dev false
```

Related Links

- 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 <export policy name>` - 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:

```
cluster1::> vserver export-policy rule delete -vserver vs0
-policyname read_only_expolicy -ruleindex 5
```

Related Links

- vserver export-policy rule setindex
- vserver export-policy rule show

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. Duplicate match strings in the same rule are not allowed. 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 <export policy name>` - 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 <Client Access Protocol>,…]` - 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

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* . If you enable NFSv4, you will not be able to apply the policy to which this rule belongs to a FlexGroup, as FlexGroups do not support NFSv4 protocol access.

[-clientmatch <text>] - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

This parameter specifies list of the match strings specifying the client or clients to which the export rule applies. You can specify the match string 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, 10.1.12.0/24
- 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 <authentication method>,…] - 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 v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- *krb5i* - 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 v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - 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 v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *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.

  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.

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 <authentication method>,…] - 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 v5.
- *krb5i* - 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 v5 with integrity service.
- *krb5p* - 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 v5 with privacy service.
- *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.

  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.

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 <authentication method>,…] - 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 v5.
- *krb5i* - 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 v5 with integrity service.
- *krb5p* - 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 v5 with privacy service.
- *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.

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.

> 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 (with value *fail*) or allowed (with value *ignore*) when the request originates from an NFS client. The default setting is `fail` . This parameter is only used if you set the NTFS UNIX security option for the Vserver to `use-export-policy` ; otherwise, it has no effect.

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode (privilege: advanced)

This parameter specifies who is authorized to change the ownership mode of a file. The default setting is `restricted` . This parameter is only used if you set the change ownership mode option for the Vserver to `use-export-policy` ; otherwise, it has no effect. The allowed values are :

- restricted - Only root user can change the ownership of the file.
- unrestricted - Non-root users may change file ownership provided the on-disk permissions allow the operation.

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 netgroups named group1 or group2 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.

```
cluster1::> vserver export-policy rule modify -vserver vs0 -policyname
default_expolicy -ruleindex 3 -protocol "nfs2,cifs"
-clientmatch "@group1, @group2" -rorule any -rwrule "ntlm,krb5" -allow
-suid true
```

Related Links

- vserver export-policy rule setindex
- vserver export-policy rule show

vserver export-policy rule remove-clientmatches

Remove list of clientmatch strings from an existing rule

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

Description

The `vserver export-policy rule remove-clientmatches` command removes a list of strings from the clientmatch field of a specified export rule in a policy. This command only operates on the clientmatch field; to modify other fields in a rule use the `vserver export-policy modify` command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy containing the export rule from which you want to remove clientmatch strings.

`-ruleindex <integer>` - Rule Index

This parameter specifies the index number of the export rule from which you want to remove clientmatch strings. To view a list of rules with their index numbers, use the vserver export-policy rule show command.

`-clientmatches <text>` - List of Clientmatch Strings to Remove

This parameter specifies list of the match strings specifying the client or clients to remove from the export rule. Match strings are removed from the clientmatch field if the match string is identical to one of the elements in the clientmatches list. If all match strings are removed from the clientmatch field the entire export rule is deleted. You can specify the match string 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, 10.1.12.0/24
- 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.

Examples

The following example removes match strings "2.2.2.2" and "3.3.3.3" from the clientmatch field of the export rule with index number 3 in an export policy named default_expolicy on a Vserver named vs0.

```
cluster1::> vserver export-policy rule remove-clientmatches -vserver vs0
-policyname default_expolicy -ruleindex 3 -clientmatches "2.2.2.2,3.3.3.3"
```

Related Links

- vserver export-policy rule show

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 <export policy name>` - 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:

```
cluster1::> vserver export-policy rule setindex -vserver vs0
-policyname read_only_policy -ruleindex 5 -newruleindex 3
```

Related Links

- 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 <export policy name>] - 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 <Client Access Protocol>,…] - 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

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>] - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

If you specify this parameter, the command displays information only about the export rules that have a clientmatch list containing all of the strings in the specified client match. You can specify the match as a list of strings 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, 10.1.12.0/24
- 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 <authentication method>,…] - 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 v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.

- *krb5i* - 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 v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - 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 v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *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.

  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.

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 <authentication method>,…] - 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.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The

effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.

- *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.

> 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.

> 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 <authentication method>,…] - 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 v5.
- *krb5i* - 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 v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - 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 v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *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.

  > 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.

  > 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.

> 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 have specified this parameter for a particular export policy rule, then the command displays information about the UNIX security options that apply to that export policy rule. The setting can either prohibit (with value *fail*) or allow (with value *ignore*) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client. If the Vserver NTFS UNIX security option is set to fail or allow for the Vserver, then this parameter is overridden.

[-ntfs-unix-security-ops-vs {fail|ignore|use-export-policy}] - Vserver NTFS Unix Security Options (privilege: advanced)

If you specify this parameter, the command displays information about the UNIX security options that apply to all volumes in this Vserver. The setting can prohibit (with value *fail*) or allow (with value *ignore*) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client, or you can set it to `use-export-policy` . If you set this parameter to `fail` or `allow` , this parameter overrides the individual UNIX security options set for the export policy rules. If you set this parameter to `use-export-policy` , the UNIX security options associated with the respective export policy rule is used.

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode (privilege: advanced)

If you have specified this parameter for a particular export policy rule, then the command displays information about the change ownership mode that applies to that export-policy rule. The setting can either allow only the root (with value *restricted*) or all users (with value *unrestricted*) to change file ownership provided the on-disk permissions allow the operation. If the Vserver change ownership mode is set to restricted or unrestricted for the Vserver, then this parameter is overridden.

[-chown-mode-vs {restricted|unrestricted|use-export-policy}] - Vserver Change Ownership Mode (privilege: advanced)

If you specify this parameter, the command displays information about the change ownership mode that applies to all volumes in this Vserver. The setting can allow only the root (with value *restricted*) or all users (with value *unrestricted*) to change ownership of the files that they own, or you can set it to `use-export-policy`. If you set this parameter to `restricted` or `unrestricted`, this parameter overrides the individual change ownership mode set for the export policy rules. If you set this parameter to `use-export-policy`, the change ownership mode associated with the respective export policy rule is used.

Examples

The following example displays information about all export rules:

```
cluster1::> vserver export-policy rule show
       Policy             Rule    Access   Client                  RO
Vserver      Name               Index   Protocol Match
Rule
------------ ------------------ ------  -------- ------------------------
------
vs0          default_expolicy   1       any      0.0.0.0/0,::0/0
any
vs0          read_only_expolicy 2       any      0.0.0.0/0
any
vs1          default_expolicy   1       any      10.10.10.10,11.11.11.11
any
vs1          test_expolicy      1       any      0.0.0.0/0
any
4 entries were displayed.
```

vserver fcp commands

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 an FCP service for a Vserver. An 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 an 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).

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver for the FCP service.

[-target-name <text>] - Target Name (privilege: advanced)

The FCP World Wide Node Name (WWNN) for the service. All FCP LIFs in the Vserver will share the specified WWNN. The format for a WWNN is "XX:XX:XX:XX:XX:XX:XX:XX" where X is a hexadecimal digit.

Unles the `force` option is also provided, the specified WWNN must be within one of the following vendor registered namespaces:

- 2X:XX:00:a0:98:XX:XX:XX
- 2X:XX:00:a0:b8:XX:XX:XX
- 2X:XX:d0:39:ea:XX:XX:XX

The user must ensure that the target name is not in use elsewhere outside the cluster. ONTAP cannot verify that the target name is unique outside the cluster if ONTAP did not generate the target name.

[-status-admin {down|up}] - Administrative Status

Specifies the administrative status of the FCP service of a Vserver. If you set this parameter to *up* , the FCP service will accept login requests from FCP initiators. If you set this parameter to *down* , FCP initiators will not be allowed to log in.

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

Allows you to specify a World Wide Node Name outside one of the known vendor registered namespaces.If you use this parameter without a value, it is set to *true* , and the command does not error when the specified WWNN is outside one of the vendor registered namespaces.

Examples

```
cluster1::> vserver fcp create -vserver vs_1
```

Creates an FCP service on Vserver *vs_1* .

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 for the FCP service.

Examples

```
cluster1::> vserver fcp delete -vserver vs_1
```

Deletes the FCP service on Vserver *vs_1* .

Related Links

- 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.

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver for the FCP service.

[-target-name <text>] - Target Name (privilege: advanced)

The FCP World Wide Node Name (WWNN) for the service. All FCP LIFs in the Vserver will share the specified WWNN. The format for a WWNN is "XX:XX:XX:XX:XX:XX:XX:XX" where X is a hexadecimal digit.

Unles the `force` option is also provided, the specified WWNN must be within one of the following vendor registered namespaces:

- 2X:XX:00:a0:98:XX:XX:XX
- 2X:XX:00:a0:b8:XX:XX:XX
- 2X:XX:d0:39:ea:XX:XX:XX

The user must ensure that the target name is not in use elsewhere outside the cluster. ONTAP cannot verify that the target name is unique outside the cluster if ONTAP did not generate the target name.

[-status-admin {down|up}] - Administrative Status

Specifies the administrative status of the FCP service of a Vserver. If you set this parameter to *up* , the FCP service accepts login requests from FCP initiators. If you set this parameter to *down* , FCP initiators cannot log in.

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

Allows you to specify a World Wide Node Name outside one of the known vendor registered namespaces.If you use this parameter without a value, it is set to *true* , and the command does not error when the specified WWNN is outside one of the vendor registered namespaces.

Examples

```
cluster1::> vserver fcp modify -vserver vs_1 -status-admin down
```

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

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
                                          Status
server    Target Name                     Admin
--------- --------------------------- ------
s0        20:00:00:a0:98:0c:b0:eb      up
s2        20:01:00:a0:98:0c:b0:eb      up
 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 for the FCP service.

Examples

```
cluster1::> vserver fcp start -vserver vs_1
   (vserver fcp start)
```

Starts FCP service for Vserver *vs_1* .

Related Links

- 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 for the FCP service.

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.

[-data-protocol {fcp|fc-nvme}] - Data Protocol

Use this parameter to display the FCP initiator that matches the data protocol that you specify.

Examples

```
cluster1::> vserver fcp initiator show
     Logical    Initiator      Initiator
 Vserver   Interface  WWNN           WWPN          Igroup
 --------- ---------- -------------- -------------
-------------------------
 vs1       vs1.fcp    2f:a2:00:a0:98:0b:56:13
                                     2f:a2:00:a0:98:0b:56:15
                                                   igroup1
```

Displays information regarding all logged in FCP initiators.

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 match 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
     Logical    Status                       Current       Current Is
Vserver    Interface  Admin/Oper WWPN             Node          Port
Home
---------- ---------- ---------- ---------------- ------------ -------
------
vs1        vs1.fcp    up/down    2f:a2:00:a0:98:0b:56:13
                                                 node1         0c
true
```

Displays all FCP interface information.

vserver fcp nameserver show

Display FCP fabric name server entries

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

Description

This command show entries in the fabric name server 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.

[-vserver <Vserver Name>] - Vserver

Use this parameter to select the Vservers that contain FCP LIFs.

[-lif <text>] - LIF Name

Use this parameter to select the FCP LIFs.

[-port-id <Hex Integer>] - Port Identifier

Use this parameter to select the assigned port identifier of the LIF.

[-unzoned <true>] - Show unzoned name server entries

Use this parameter to show unzoned name server information.

[-port-type <text>] - Port Type

Use this parameter to select the port type of the LIF.

[-port-wwn <text>] - Port WWN

Use this parameter to select World Wide Port Name (WWPN) of the LIF.

[-fabric-port-wwn <text>] - Fabric Port WWN

Use this parameter to select the fabric World Wide Port Name (WWPN) of the lif.

[-node-wwn <text>] - Node WWN

Use this parameter to select the World Wide Node Name (WWNN) of the LIF.

[-service-class <text>] - Service Class

Use this parameter to select the registered class of services as defined in the FC-FS standard.

[-fc4-type <text>] - FC4 Type

Use this parameter to select the registered FC4 type.

[-switch-port <text>] - Switch Port

Use this parameter to select the name of switch port connected to target array.

Examples

```
cluster1::> vserver fcp nameserver show
                                                        Port     Port
FC4
        Vserver:Lif         Node WWN, Port WWN          Id       Type
Type
        ------------------- ----------------------- -------- ------------
------------
        vs1 :lif1
                            20:00:00:a0:98:55:73:38
                            20:01:00:a0:98:55:73:38   8130561  N-Port
FCP
                            20:00:00:90:fa:73:12:dd
                            10:00:00:90:fa:73:12:dd   8194560  N-Port
        vs1 :lif2
                            20:00:00:90:fa:94:29:ee
                            10:00:00:90:fa:94:29:ee   8201984  N-Port
FCP
        3 entries were displayed.
```

vserver fcp ping-igroup show

Ping FCP by Igroup

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

Description

This command performs a connectivity check (ping) between the FCP initiators of an igroup and the FCP LIFs for which they are configured.

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 select the Vservers that contain initiators and FCP LIFs.

[-igroup <text>] - Igroup Name

Use this parameter to select the FCP initiators that belong to the specified igroup and FCP LIFs that belong to the portset that is bound to the igroup. If the igroup is not bound to a portset, then the default portset (all FCP LIFs in the Vserver), is used.

[-wwpn <text>] - FCP initiator WWPN

Use this parameter to select the FCP initiator WWPN.

[-lif <text>] - LIF Name

Use this parameter to limit the test to a subset of the FCP LIFs available for the igroup.

[-portset <text>] - Portset

Use this parameter to select igroups bound to the specified portset.

[-node <nodename>] - Node

Use this parameter to select the nodes that contain the specified FCP LIFs.

[-status {unknown|reachable|not-reachable|not-zoned|cannot-ping-same-wwpn|fcp-service-busy|lif-is-down|zone-info-not-available}] - Ping Status

Use this parameter to select the status of FCP ping command.

[-ext-status {logged-in|not-logged_in|not-in-fabric|not-in-same-zone|fabric-info-not-available}] - Extended Status

Use this parameter to select the extended status of FCP ping command.

[-check-fabric <true>] - Query Fabric Records (privilege: advanced)

Use this parameter to query the unzoned name server for the FCP initiator WWPN.

Examples

```
cluster1::> vserver fcp ping-igroup show
          Igroup                     Node       Logical   Ping
Extended
Vserver   Name        WWPN           Name       Interface Status
Status
--------- ----------- -------------- ---------- --------- ----------
-----------
vserver_1
          igroup_1    c0:03:ff:e4:70:06:00:e4
                                     node_1
                                                lif_1     reachable  wwpn-
logged-in
          igroup_1    c0:03:ff:e4:70:06:00:e6
                                     node_2
                                                lif_2     not-zoned  -
2 entries were displayed.
```

vserver fcp ping-initiator show

Ping FCP initiator

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

Description

This command performs a connectivity check (ping) between FCP initiators and FCP 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 select the Vservers that contain FCP initiators and FCP LIFs.

-wwpn <text> - Remote WWPN

Use this parameter to select the remote WWPN (most likely, FCP initiator).

[-lif <text>] - LIF Name

Use this parameter to limit the test to a subset of the FCP LIFs available for the igroup.

[-check-fabric <true>] - Query Fabric Records (privilege: advanced)

Use this parameter to query the unzoned name server for the FCP initiator WWPN.

[-node <nodename>] - Node

Use this parameter to select the nodes that contain the specified FCP LIFs.

[-status {unknown|reachable|not-reachable|not-zoned|cannot-ping-same-wwpn|fcp-service-busy|lif-is-down|zone-info-not-available}] - Ping Status

Use this parameter to select the result of FCP ping command.

[-ext-status {logged-in|not-logged_in|not-in-fabric|not-in-same-zone|fabric-info-not-available}] - Extended Status

Use this parameter to select the extended result of FCP ping command.

Examples

```
cluster1::> vserver fcp ping-initiator show
                          Node       Logical    Ping      Extended
Vserver   WWPN            Name       Interface Status    Status
--------- --------------- ---------- --------- --------- -----------
vserver_1
          c0:03:ff:e4:70:06:00:e4
                          node_1
                                     lif_1     reachable wwpn-logged-in
          c0:03:ff:e4:70:06:00:e6
                          node_2
                                     lif_2     not-zoned -
2 entries were displayed.
```

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. The administration status of logical interface must be down before you can change the WWPN.

Use the network interface modify to change the administration status of the logical interface.

Parameters

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

Specifies the Vserver.

-lif <lif-name> - Logical Interface (privilege: advanced)

Specifies the logical interface to which you want to assign a new WWPN.

-wwpn <text> - FCP Adapter WWPN (privilege: advanced)

Specifies the WWPN that you want to change.

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

Allows you to use a WWPN that is not in the format 2X:XX:0a:09:80:XX:XX:XX when set to true. If you use this parameter without a value, it is set to true, and the command does not prompt you when the WWNN does not follow this format.

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.

Related Links

- 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
           Logical
Vserver    Interface      WWPN
---------  -------------- -------------------------
vs_a       vs_a.fcp       2f:a2:00:a0:98:0b:56:13
vs_io1     vs_io1.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 topology show

Show FCP topology interconnect elements

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

Description

Show FCP topology interconnect elements

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 select the interconnect elements for the specified Vservers.

[-lif <text>] - LIF Name

Use this parameter to select the interconnect elements for the specified FCP LIFs.

[-domain-id <integer>] - Domain Identifier

Use this parameter to select the interconnect elements with the specified domain identifier

[-logical-name <text>] - Logical Name

Use this parameter to select the interconnect elements with the specified logical name

[-vendor <text>] - Vendor

Use this parameter to select the interconnect elements with the specified vendor

[-release <text>] - Release

Use this parameter to select the interconnect elements with the specified release

[-wwn <text>] - World Wide Name

Use this parameter to select the interconnect elements with the specified World Wide Name

[-port-count <integer>] - Port Count

Use this parameter to select the interconnect elements with the specified port count

Examples

```
cluster1::> vserver fcp topology show
                        Domain Logical
Port
Vserver Lif Name        Id     Name                WWN
Count
------- ------------- ------ ------------------- ----------------------
-----
vs1     lif1
                        98     ssan-fc0e-fit-01    20:05:00:05:73:bd:a3:01
15
                        99     ssan-fc0e-d38       20:05:8c:60:4f:04:f1:01
11
                        112    ssan-fc0e-5         20:05:00:0d:ec:ca:0b:41
19
                        119    ssan-fc0e-core-a    20:05:54:7f:ee:02:c1:01
18
                        159    ssan-fc0e-7         20:05:00:05:9b:24:6e:c1
38
                        169    sdev-fc0e-gg26      20:05:54:7f:ee:31:06:81
53
                        174    ssan-fc0e-d46       20:05:00:05:9b:7d:f8:01
16
                        177    ssan-fc0e-e49       20:05:54:7f:ee:ef:1c:81
19
                        180    ssan-fc0e-d40       20:05:00:05:9b:79:a3:c1
20
vs1     lif2
                        229    ssan-fc0e-6         20:05:00:05:73:c8:8f:01
33
                        233    ssan-fc0e-e45       20:05:54:7f:ee:a0:67:01
8
11 entries were displayed.
```

The example above show FCP topology interconnect information for the cluster.

vserver fcp wwn blacklist show

Displays the blacklisted WWNs

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

Description

This command displays WWNs that have been blacklisted from re-use.

A blacklisted WWN is a WWN that is prohibited for use as either a fiber channel protocol service WWNN or a fiber channel data LIF WWPN.

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.

[-wwn <text>] - World Wide Name (privilege: advanced)

Selects the blacklisted WWNs that match the parameter value.

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

Selects the blacklisted WWNs that were previously assigned to the Vserver(s) that match the parameter value.

Examples

```
cluster1::> vserver fcp wwn blacklist show
        WWN                      Vserver
        ------------------------ ----------
        01:02:03:04:05:06:07:08 vs1
        01:02:03:04:05:06:07:09 vs1
        2 entries were displayed.
```

Displays the blacklisted WWNs.

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.

{ -a, -alias <text>,… - Initiator WWPN Alias

Specifies the alias of the WWPN that you want to remove.

| -w, -wwpn <FC WWN> - 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 is a case-sensitive name that must contain one to 32 characters. Spaces are not allowed.

Parameters

-vserver <Vserver Name> - Vserver Name
Specifies the Vserver.

-a, -alias <text> - Initiator WWPN Alias
Specifies the alias of the WWPN.

-w, -wwpn <FC WWN> - Initiator WWPN
Specifies the WWPN.

[-f, -force <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::> vserver fcp wwpn-alias set -vserver 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).

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.

[-a, -alias <text>] - Initiator WWPN Alias

Use this parameter to display the WWPN that matches the alias that you specify.

[-w, -wwpn <FC WWN>] - Initiator WWPN

Use this parameter to display a list of aliases that match the WWPN that you specify.

Examples

```
cluster1::> vserver fcp wwpn-alias show
    Initiator               Initiator
Vserver   WWPN                    Alias
--------- ----------------------- ------------------
vs1       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 vs1.

Related Links

- lun igroup show
- lun igroup create
- lun igroup add
- lun igroup remove
- vserver fcp show

vserver fpolicy commands

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.

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.

```
cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  ------
--------
vs1.example.com         vs1_pol                                 -  off
native
vs2.example.com         vs2_pol                                 5  on
external
2 entries were displayed.

cluster1::> vserver fpolicy disable -vserver vs2.example.com -policy-name
vs2_pol

cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol                                 -  off
native
vs2.example.com         vs2_pol                                 -  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 have a higher priority than policies for any other engine, regardless of the sequence number assigned to them.

Events on FlexGroup volumes do not notify the FPolicy server.

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 that is assigned to the policy.

Examples

The following command enables an FPolicy policy:

```
cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  ------
--------
vs1.example.com         vs1_pol                                 -  off
native
vs2.example.com         vs2_pol                                 -  off
external
2 entries were displayed.
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol                                 -  off
native
vs2.example.com         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

The FPolicy event and external engine must be attached to the FPolicy policy.

The FPolicy policy should be enabled.

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.

```
cluster1::> vserver fpolicy engine-connect -node FPolicy-01 -vserver
vs1.example.com -policy-name p -server 1.1.1.1
cluster1::> vserver fpolicy show
  FPolicy                                                    Server-
Server-
  Vserver         Policy        Node          Server           status
type
  --------------- ------------- ------------ -----------------
-------------- -----------
  vs1.example.com 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.

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.

```
cluster1::> vserver fpolicy engine-disconnect -node FPolicy-01 -vserver
vs1.example.com -policy-name p -server 1.1.1.1
cluster1::> vserver fpolicy show
 FPolicy                                                    Server-
Server-
 Vserver         Policy        Node         Server           status
type
 --------------- ------------- ------------ -----------------
-------------- -----------
 vs1.example.com 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.

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.

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name                     Priority

----------------------- ------------------------------- ----------
vs1.example.com         pol_native                      native
vs1.example.com         pol_native2                     native
vs1.example.com         pol1                            2
vs1.example.com         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.

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).

```
cluster1::> vserver fpolicy show-engine
 FPolicy                                                    Server-
Server-
 Vserver         Policy        Node         Server           status
type
 --------------- ------------- ------------ -----------------
-------------- -----------
 vs2.example.com vs2_pol       FPolicy-01   9.9.9.9          connected
primary
 vs1.example.com 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).

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
 node       vserver         policy-name server
 ---------- --------------- ----------- -------
 FPolicy-01 vs1.example.com vs1_pol     1.1.1.1
```

This example displays information about an FPolicy server.

```
cluster1::> vserver fpolicy show-engine -server 10.72.204.118 -instance
Node: fpol-01
                                Vserver: vserver_1.example.com
                                 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-passthrough-read-connection

Display connection status for FPolicy passthrough-read

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

Description

The `vserver fpolicy show-passthrough-read-connection` command displays the status of the passthrough-read connection from all FPolicy servers. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. If you do not specify any parameters, the command displays following information about the passthrough-read connection from FPolicy servers:

- Vserver name
- FPolicy policy name
- Node name
- FPolicy server IP address
- Passthrough-read connection status

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields.

- Session ID of the control channel

- Time passthrough-read channel was connected
- Time passthrough-read channel was disconnected
- Reason for passthrough-read channel disconnection

You can specify the `-instance` parameter to display information for all passthrough-read connections in the 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.

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

If you specify this parameter, the command displays information only about the passthrough-read connections on the specified node.

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, the command displays information only about the passthrough-read connections for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the passthrough-read connections that are attached with the specified FPolicy policy.

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the passthrough-read connections from the specified FPolicy server.

[-control-session-id <text>] - Session ID of the Control Channel

If you specify this parameter, the command displays information only about the passthrough-read connections that are connected with the specified control session ID. The passthrough-read connection is attached to a control connection that has a unique control session ID.

[-server-status <Status of fpolicy passthrough-read connection>] - Server Status

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified status.

[-connected-since <MM/DD/YYYY HH:MM:SS>] - Time Channel Was Connected

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified connection time.

[-disconnected-since <MM/DD/YYYY HH:MM:SS>] - Time Channel Was Disconnected

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified disconnection time.

[-disconnect-reason <Reason for fpolicy passthrough-read disconnection>] - Reason for Disconnection

If you specify this parameter, the command displays information only about the passthrough-read connections that are disconnected because of the specified disconnect reason.

Examples

This example displays information about passthrough-read connections from all FPolicy servers.

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ----------- -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
2 entries were displayed.
```

This example displays information about passthrough-read connections from all connected FPolicy servers.

```
cluster1::> vserver fpolicy show-passthrough-read-connection -server
-status connected
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ----------- -----------------
--------------
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

This example displays information about passthrough-read connections from FPolicy servers configured in an FPolicy policy.

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance
Node: FPolicy-01
                                       Vserver: vserver_1.example.com
                                        Policy: pol_cifs_1
                                        Server: 2.2.2.2
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                  Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

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.

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.

```
cluster1::> vserver fpolicy show
                                                                 Sequence
            Vserver                 Policy Name                    Number
Status      Engine
            ----------------------- -------------------------- --------
---------   ---------
            FPolicy                 cserver_policy             -
off         eng1
            vs1.example.com         v1p1                       -
off         eng2
            vs1.example.com         v1p2                       -
off         native
            vs1.example.com         v1p3                       -
off         native
            vs1.example.com         cserver_policy             -
off         eng1
            vs2.example.com         v1p1                       3
on          native
            vs2.example.com         v1p2                       1
on          eng3
            vs2.example.com         cserver_policy             2
on          eng1
            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.

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.

[-is-passthrough-read-enabled {true|false}] - Is Passthrough Read Enabled

This parameter specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are the files which have been moved to secondary storage. If passthrough-read is enabled, the FPolicy server provides the data for the file over a separate channel instead of restoring the file to primary storage. By default, this parameter is *false* .

Examples

The following example creates an FPolicy policy.

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com -policy
-name vs1_pol -events cserver_evt,v1e1
          -engine native -is-mandatory true -allow-privileged-access no
-is-passthrough-read-enabled false

cluster1::> vserver fpolicy policy show -vserver vs1.example.com -policy
-name vs1_pol
Vserver: vs1.example.com
                    Policy Name: vs1_pol
              Events to Monitor: cserver_evt, v1e1
                 FPolicy Engine: native
Is Mandatory Screening Required: true
        Allow Privileged Access: no
User Name for Privileged Access: -
    Is Passthrough Read Enabled: false
```

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.

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.

```
cluster1::> vserver fpolicy policy delete -vserver vs1.example.com -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.

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.

`[-is-passthrough-read-enabled {true|false}]` - Is Passthrough Read Enabled

This parameter specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are the files which have been moved to secondary storage. If passthrough-read is enabled, the FPolicy server provides the data for the file over a separate channel instead of restoring the file to primary storage. By default, this parameter is *`false`* .

Examples

The following example modifies an FPolicy policy.

```
cluster1::> vserver fpolicy policy modify -vserver vs1.example.com -policy
-name vs1_pol -events cserver_evt,v1e1
          -engine native -is-mandatory true -allow-privileged-access no
-is-passthrough-read-enabled false

cluster1::> vserver fpolicy policy show -vserver vs1.example.com -policy
-name vs1_pol
Vserver: vs1.example.com
                    Policy Name: vs1_pol
              Events to Monitor: cserver_evt, v1e1
                 FPolicy Engine: native
Is Mandatory Screening Required: true
        Allow Privileged Access: no
User Name for Privileged Access: -
    Is Passthrough Read Enabled: false
```

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.

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.

[-is-passthrough-read-enabled {true|false}] - Is Passthrough Read Enabled

If you specify this parameter, the command displays information only about the FPolicy policies that use the specified passthrough-read setting.

Examples

The following example displays the information about FPolicy policies on the cluster using the `vserver fpolicy policy show` command.

```
cluster1::> vserver fpolicy policy show
Vserver         Policy       Events     Engine         Is Mandatory
PrivAccess
--------------- -----------  ---------- -------------  ------------
----------
Cluster         cserver_pol  cserver_   cserver_eng    true          yes
                             evt
vs1.example.com p            r          n              true          no
vs1.example.com cserver_pol  cserver_   cserver_eng    true          yes
                             evt
vs2.example.com cserver_pol  cserver_   cserver_eng    true          yes
                             evt
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".

```
cluster1::> vserver fpolicy policy show -fields policy-name -allow
-privileged-access yes
vserver         policy-name
--------------- -----------
Cluster         cserver_pol
vs1.example.com cserver_pol
vs2.example.com 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.

Three parameters have dependency rules: `-protocol` , `-files-operations` and `-filters` . The following combinations are supported:

- Both `-protocol` and `-file-operations`
- All of `-protocol` , `-file-operations` and `-filters`
- Specify none of three

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.

> 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.

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.
- `_ close-with-read _` - Filter the client request for close with read.
- `_ first-read _` - Filter the client requests for the first-read. When this filter is used for CIFS events, the first-read request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping -duration` configurations determine the first read-request for which FPolicy processing is done.
- `_ first-write _` - Filter the client requests for the first-write. When this filter is used for CIFS events, the first-write request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io -grouping-duration` configurations determine the first-write request for which FPolicy processing is done.
- `_ 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.
- `_ setattr-with-owner-change _` - Filter the client setattr requests for changing owner of a file or directory.
- `_ setattr-with-group-change _` - Filter the client setattr requests for changing group of a file or directory.
- `_ setattr-with-sacl-change _` - Filter the client setattr requests for changing sacl on a file or directory.
- `_ setattr-with-dacl-change _` - Filter the client setattr requests for changing dacl on a file or directory.
- `_ setattr-with-modify-time-change _` - Filter the client setattr requests for changing the modification time of a file or directory.
- `_ setattr-with-access-time-change _` - Filter the client setattr requests for changing the access time of a file or directory.
- `_ setattr-with-creation-time-change _` - Filter the client setattr requests for changing the

creation time of a file or directory.

- _ setattr-with-mode-change _ - Filter the client setattr requests for changing the mode bits on a file or directory.
- _ setattr-with-size-change _ - Filter the client setattr requests for changing the size of a file.
- _ setattr-with-allocation-size-change _ - Filter the client setattr requests for changing the allocation size of a file.
- _ exclude-directory _ - Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.

If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

If the client sends multiple read/write requests simultaneously for the same file, then the first-read and first-write filters can result in more than one FPolicy notification.

`[-volume-operation {true|false}]` - Send Volume Operation Notifications

This parameter specifies whether volume operations generate notifications for the FPolicy event. If this field is set to *`true`* then FPolicy sends notifications when volumes are mounted or unmounted. By default, it is *`false`*.

Examples

The following example creates an FPolicy event.

```
cluster1::> vserver fpolicy policy event create -vserver vs1.example.com
-event-name cifs_event -protocol cifs
                                                                  -file
-operations open,close,read,write -filters first-read,offline-bit
                                                                  -volume
-operation true
cluster1::> vserver fpolicy policy event show -vserver vs1.example.com
-event-name cifs_event
Vserver: vs1.example.com
                  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, close-with-read, exclude-directory
    create     : monitor-ads, offline-bit
    create_dir : none
    delete     : monitor-ads, offline-bit
    delete_dir : none
    getattr    : offline-bit, exclude-directory
    open       : monitor-ads, offline-bit, open-with-delete-intent, open-
with-write-intent,
                 exclude-directory
    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 : none
    setattr    : offline-bit, monitor-ads, setattr-with-owner-change,
                 setattr-with-group-change, setattr-with-sacl-change,
                 setattr-with-dacl-change, setattr-with-modify-time-
change,
                 setattr-with-access-time-change, setattr-with-creation-
time-change,
                 setattr-with-size-change, setattr-with-allocation-size-
change,
                 exclude-directory
```

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 : none
     delete     : offline-bit
     delete_dir : none
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-mode-change, setattr-with-size-change,
exclude-directory
     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, exclude-directory
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     getattr    : offline-bit, exclude-directory
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     open       : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-sacl-change, setattr-with-dacl-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-size-change, exclude-directory
     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.

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.

```
cluster1::> vserver fpolicy policy event delete  -vserver vs1.example.com
-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.

Three parameters have dependency rules: `-protocol` , `-files-operations` and `-filters` . The following combinations are supported:

- Both `-protocol` and `-file-operations`
- All of `-protocol` , `-file-operations` and `-filters`
- Specify none of three

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.

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.

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.
- `_close-with-read_` - Filter the client request for close with read.
- `_first-read_` - Filter the client requests for the first-read. When this filter is used for CIFS events, the first-read request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` configurations determine the first read-request for which FPolicy processing is done.

- _ `first-write` _ - Filter the client requests for the first-write. When this filter is used for CIFS events, the first-write request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` configurations determine the first-write request for which FPolicy processing is done.
- _ `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.
- _ `setattr-with-owner-change` _ - Filter the client setattr requests for changing owner of a file or directory.
- _ `setattr-with-group-change` _ - Filter the client setattr requests for changing group of a file or directory.
- _ `setattr-with-sacl-change` _ - Filter the client setattr requests for changing sacl on a file or directory.
- _ `setattr-with-dacl-change` _ - Filter the client setattr requests for changing dacl on a file or directory.
- _ `setattr-with-modify-time-change` _ - Filter the client setattr requests for changing the modification time of a file or directory.
- _ `setattr-with-access-time-change` _ - Filter the client setattr requests for changing the access time of a file or directory.
- _ `setattr-with-creation-time-change` _ - Filter the client setattr requests for changing the creation time of a file or directory.
- _ `setattr-with-mode-change` _ - Filter the client setattr requests for changing the mode bits on a file or directory.
- _ `setattr-with-size-change` _ - Filter the client setattr requests for changing the size of a file.
- _ `setattr-with-allocation-size-change` _ - Filter the client setattr requests for changing the allocation size of a file.
- _ `exclude-directory` _ - Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.

If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

If the client sends multiple read/write requests simultaneously for the same file, then the first-read and first-write filters can result in more than one FPolicy notification.

[-volume-operation {true|false}] - Send Volume Operation Notifications

This parameter specifies whether volume operations generate notifications for the FPolicy event. If this field is set to *true* then FPolicy sends notifications when volumes are mounted or unmounted. By default, it is *false*.

Examples

The following example modifies an FPolicy event.

```
cluster1::> vserver fpolicy policy event modify -vserver vs1.example.com
-event-name cifs_event -protocol cifs
                                                                  -file
-operations open,close,read,write -filters first-read,offline-bit
                                                                  -volume
-operation true
cluster1::> vserver fpolicy policy event show -vserver vs1.example.com
-event-name cifs_event
Vserver: vs1.example.com
                  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, close-with-read, exclude-directory
    create     : monitor-ads, offline-bit
    create_dir : none
    delete     : monitor-ads, offline-bit
    delete_dir : none
    getattr    : offline-bit, exclude-directory
    open       : monitor-ads, offline-bit, open-with-delete-intent, open-
with-write-intent,
                 exclude-directory
    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 : none
    setattr    : offline-bit, monitor-ads, setattr-with-owner-change,
                 setattr-with-group-change, setattr-with-sacl-change,
                 setattr-with-dacl-change, setattr-with-modify-time-
change,
                 setattr-with-access-time-change, setattr-with-creation-
time-change,
                 setattr-with-size-change, setattr-with-allocation-size-
change,
                 exclude-directory
```

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 : none
     delete     : offline-bit
     delete_dir : none
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-mode-change, setattr-with-size-change,
exclude-directory
     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, exclude-directory
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     getattr    : offline-bit, exclude-directory
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     open       : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-sacl-change, setattr-with-dacl-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-size-change, exclude-directory
     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.

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}] - Send Volume Operation Notifications

If this field is set to *`true`* , then FPolicy displays information about those events for which it sends notifications when volumes are mounted or unmounted. If you set this parameter to *`true`* , the command displays information about events where the `-volume-operation` parameter is set *`true`* and volume operations such as mount and unmount are monitored. If you set this parameter to *`false`* , the command displays information about events where volume operations are not monitored.

Examples

The following example displays the information about all Vserver FPolicy policy events.

```
cluster1::> vserver fpolicy policy event show
                                Event                          File
Volume
                Vserver         Name                Protocols Operations
Filters      Operation
                --------------- ------------------ --------- -------------
------------ ------------
                Cluster         cserver_evt        cifs      open, close,
first-write, true
                                                              read, write
first-read
                vs1.example.com cserver_evt        cifs      open, close,
first-write, true
                                                              read, write
first-read
                vs1.example.com v1e1               cifs      open, read
first-read   -
                vs1.example.com v1e2               cifs      open
-            false
                vs1.example.com v1e3               nfsv4     open
-            true
                vs2.example.com cserver_evt        cifs      open, close,
first-write, true
                                                              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.

```
cluster1::> vserver fpolicy policy event show -fields event-name -protocol
cifs -volume-operation false
               vserver         event-name
               --------------- ----------
               vs1.example.com v1e2
```

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.

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.

[-recv-buffer-size <integer>] - Receive Buffer Size (privilege: advanced)

This parameter specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.

[-send-buffer-size <integer>] - Send Buffer Size (privilege: advanced)

This parameter specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-defualt value to set the size (in bytes) of the send buffer.

[-session-timeout <[<integer>h][<integer>m][<integer>s]>] - Session ID Purge Timeout During Reconnection (privilege: advanced)

This parameter specifies the interval after which a new session ID is sent to the FPolicy server during reconnection attempts. The value for this field must be between 0s and 200s. The default value is set to 10 seconds. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.

[-is-resiliency-enabled {true|false}] - Is Resiliency Feature Enabled

This parameter specifies whether the resiliency feature is enabled. When this parameter is set to *`true`* and all the primary and secondary servers are down, or no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified `-resiliency-directory -path` . To deny the file access events from being stored under these circumstances, set this parameter to *`false`* . By default, it is *`false`* .

[-resiliency-max-retention-duration <[<integer>h][<integer>m][<integer>s]>] - Maximum Notification Retention Duration

This parameter specifies the duration for which the notifications are written to files inside the storage controller during network outage. The value for this field must be between 0s and 600s. By default, it is set to 180s.

[-resiliency-directory-path <text>] - Directory for Notification Storage

This parameter specifies the directory path under the `-vserver` namespace, where notifications are stored in the files whenever network outage happens.

Examples

The following example creates an FPolicy external engine.

```
cluster1::> vserver fpolicy policy external-engine create -vserver
vs1.example.com -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

cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               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
```

Related Links

- 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.

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.

```
cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               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

cluster1::> vserver fpolicy policy external-engine delete -vserver
vs1.example.com -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.

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.

[-recv-buffer-size <integer>] - Receive Buffer Size (privilege: advanced)

This parameter specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.

[-send-buffer-size <integer>] - Send Buffer Size (privilege: advanced)

This parameter specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-defualt value to set the size (in bytes) of the send buffer.

[-session-timeout <[<integer>h][<integer>m][<integer>s]>] - Session ID Purge Timeout During Reconnection (privilege: advanced)

This parameter specifies the interval after which a new session ID is sent to the FPolicy server during reconnection attempts. The value for this field must be between 0s and 200s. The default value is set to 10 seconds. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.

[-is-resiliency-enabled {true|false}] - Is Resiliency Feature Enabled

This parameter specifies whether the resiliency feature is enabled. When this parameter is set to *`true`* and all the primary and secondary servers are down, or no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified `-resiliency-directory -path` . To deny the file access events from being stored under these circumstances, set this parameter to *`false`* . By default, it is *`false`* .

[-resiliency-max-retention-duration <[<integer>h][<integer>m][<integer>s]>] - Maximum Notification Retention Duration

This parameter specifies the duration for which the notifications are written to files inside the storage controller during network outage. The value for this field must be between 0s and 600s. By default, it is set to 180s.

[-resiliency-directory-path <text>] - Directory for Notification Storage

This parameter specifies the directory path under the `-vserver` namespace, where notifications are stored in the files whenever network outage happens.

Examples

The following example modifies an FPolicy external engine.

```
cluster1::> vserver fpolicy policy external-engine modify -vserver
vs1.example.com -engine-name new_engine -primary-servers 1.1.1.1 -port 10
-secondary-servers 2.2.2.2

cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               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
```

Related Links

- 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.

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. FPolicy external engines that the cluster administrator creates are visible in all Vservers.

[-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.

[-recv-buffer-size <integer>] - Receive Buffer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified receive buffer size.

[-send-buffer-size <integer>] - Send Buffer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified send buffer size.

[-session-timeout <[<integer>h][<integer>m][<integer>s]>] - Session ID Purge Timeout During Reconnection (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified session timeout.

[-is-resiliency-enabled {true|false}] - Is Resiliency Feature Enabled

If you specify this parameter set to *true* , the command displays information only about the FPolicy external engine or engines that has the resiliency feature enabled.

[-resiliency-max-retention-duration <[<integer>h][<integer>m][<integer>s]>] - Maximum Notification Retention Duration

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified network outage duration.

[-resiliency-directory-path <text>] - Directory for Notification Storage

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified directory path.

Examples

The following example displays the information about the configured external engines using the `vserver fpolicy policy external-engine show` command.

```
cluster1::> vserver fpolicy policy external-engine show
                            Primary           Secondary
External
 Vserver         Engine       Servers           Servers             Port
Engine Type
 --------------- -----------  ----------------- ----------------- ------
-----------
 Cluster         cserver_eng  9.9.9.9           -                     9
synchronous
 vs1.example.com cserver_eng  9.9.9.9           -                     9
synchronous
 vs1.example.com v1n1         1.1.1.1           2.2.2.2               1
synchronous
 vs2.example.com cserver_eng  9.9.9.9           -                     9
synchronous
 vs2.example.com 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.

```
cluster1::> vserver fpolicy policy external-engine show -fields engine-
name -port 9
 vserver         engine-name
 --------------- -----------
 Cluster         cserver_eng
 vs1.example.com cserver_eng
 vs2.example.com 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.

> 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.

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 "*".

> 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 "*".

> 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 "*".

> 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 "?".

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. By default, it is *false* .

[-is-monitoring-of-objects-with-no-extension-enabled {true|false}] - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

This parameter specifies whether the extension checks apply to objects with no extension as well. If this parameter is set to true, the objects with no extension are also monitored along with the objects with extension. By default, it is *false* .

This parameter is ignored when file-extensions-to-include and file-extensions-to-exclude lists are empty.

Examples

The following example creates an FPolicy policy scope.

```
cluster1::> vserver fpolicy policy scope create   -vserver vs1.example.com
                                                          -policy-name
vs1_pol
                                                          -file
-extensions-to-include flv,wmv,mp3,mp4
                                                          -file
-extensions-to-exclude cpp,c,h,txt
cluster1::> vserver fpolicy policy scope show
            Vserver           Policy              Extensions
Extensions
            Name              Name                Included
Excluded
            ----------------- ------------------- --------------------
--------------------
            Cluster           cserver_pol         txt
mp3, wmv
            vs1.example.com   vs1_pol             flv, wmv, mp3, mp4
cpp, c, h, txt
            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.

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.

```
cluster1::> vserver fpolicy policy scope delete -vserver vs1.example.com
-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.

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 "*".

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 "*".

> 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 "*".

> 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 "?".

> 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. By default, it is *false* .

[-is-monitoring-of-objects-with-no-extension-enabled {true|false}] - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

This parameter specifies whether the extension checks apply to objects with no extension as well. If this parameter is set to true, the objects with no extension are also monitored along with the objects with extension. By default, it is *false* .

This parameter is ignored when file-extensions-to-include and file-extensions-to-exclude lists are empty.

Examples

The following example modifies an FPolicy policy scope.

```
cluster1::> vserver fpolicy policy scope modify   -vserver vs1.example.com
                                                            -policy-name
vs1_pol
                                                            -file
-extensions-to-include flv,wmv,mp3,mp4
                                                            -file
-extensions-to-exclude cpp,c,h,txt
cluster1::> vserver fpolicy policy scope show
            Vserver           Policy              Extensions
Extensions
            Name              Name                Included
Excluded
            ----------------- ------------------- --------------------
--------------------
            Cluster           cserver_pol         txt
mp3, wmv
            vs1.example.com   vs1_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 use 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 extention check on directories is enabled
- Whether monitoring of objects with no extension 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.

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.

[-is-monitoring-of-objects-with-no-extension-enabled {true|false}] - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified monitoring of objects with no extension setting. If set to true, the command displays information about scope of policy or policies for which monitoring of objects with no extension is enabled.

Examples

The following example displays scope information about FPolicy policies.

```
cluster1::> vserver fpolicy policy scope show
         Vserver           Policy              Extensions
Extensions
         Name              Name                Included
Excluded
         ----------------- ------------------- --------------------
-------------------
         Cluster           cserver_pol         -                    -
         vs1.example.com   p                   -                    -
         vs1.example.com   vs1_pol             mp3                  -
         3 entries were displayed.
```

vserver http-proxy commands

vserver http-proxy create

Create a HTTP Proxy configuration

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

Description

The `vserver http-proxy create` command creates an HTTP proxy configuration for a Vserver.

Parameters

{ -vserver <vserver> - Vserver
Use this parameter to specify the Vserver on which the HTTP proxy configuration is to be created.

Note that `-vserver` and `-ipspace` are mutually exclusive options.

| [-ipspace <text>] - Ipspace }
Use this parameter to specify the IPspace on which the HTTP proxy configuration is to be created. The proxy is created on the system Vserver of that IPspace.

Note that `-vserver` and `-ipspace` are mutually exclusive options.

-server <text> - Proxy Server
Use this parameter to specify the Fully Qualified Domain Name or IP address of the proxy server.

-port <integer> - Port
Use this parameter to specify the port number on which the HTTP proxy service is configured on the proxy server.

-is-auth-enabled {true|false} - Authentication Enabled
Use this parameter to specify if authentication is enabled to connect to the HTTP proxy server. By default it is set to false. When set to true, username and password will be prompted.

[-skip-config-validation <true>] - Skip the config validation

Use this parameter to skip the HTTP proxy configuration validation.

The proxy configuration is validated to verify that the specified server is reachable and is providing an HTTP proxy service on the specified port.

The validation fails in the following cases:

- The server is not reachable.
- The specified port is invalid.
- HTTP proxy service is not configured on the specified server and port.
- Route or LIF does not exist.

Examples

The following example creates an HTTP proxy configuration for the Vserver vs0 with Fully Qualified Domain Name as input for the `-server` parameter:

```
cluster1::*> vserver http-proxy create -vserver vs0 -server example.com
-port 222
```

The following example creates an HTTP proxy configuration with the IP address as input for the `-server` parameter:

```
cluster1::*> vserver http-proxy create -vserver vs0 -server 192.168.0.0
-port 222
```

The following example creates an HTTP proxy configuration with `-skip-config-validation` set to true:

```
cluster1::*> vserver http-proxy create -vserver vs0 -server 192.168.0.0
-port 222 -skip-config-validation
```

The following example creates an HTTP proxy configuration with the IPspace specified and not the Vserver name:

```
cluster1::*> vserver http-proxy create -ipspace default -server
192.168.0.0 -port 222
```

The following example creates an HTTP proxy configuration with authentication enabled:

```
cluster1::*> vserver http-proxy create -ipspace default -server
192.168.0.0 -port 222 -is-auth-enabled true

Enter the user name: test

Enter the password:
```

vserver http-proxy delete

Remove a HTTP Proxy configuration

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

Description

The `vserver http-proxy delete` command deletes an HTTP proxy configuration.

Parameters

`-vserver <vserver>` - Vserver
Use this parameter to specify the Vserver for which the HTTP proxy configuration is to be deleted.

Examples

The following example deletes the HTTP proxy configuration for the Vserver vs0:

```
cluster1::*> vserver http-proxy delete -vserver vs0
```

vserver http-proxy modify

Change a HTTP Proxy configuration

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

Description

The `vserver http-proxy modify` command modifies an HTTP proxy configuration of a Vserver.

Parameters

{ `-vserver <vserver>` - Vserver
Use this parameter to specify the Vserver for which the HTTP proxy server configuration is to be modified.

Note that `-vserver` and `-ipspace` are mutually exclusive options.

| `[-ipspace <text>]` - Ipspace }
Use this parameter to specify the IPspace for which the HTTP proxy server configuration is to be modified.

Note that `-vserver` and `-ipspace` are mutually exclusive options.

[-server <text>] - Proxy Server

Use this parameter to specify the Fully Qualified Domain Name or IP address of the proxy server.

[-port <integer>] - Port

Use this parameter to specify the port number on which the HTTP proxy service is configured on the proxy server.

[-is-auth-enabled {true|false}] - Authentication Enabled

Use this parameter to specify if authentication is enabled to connect to the HTTP proxy server. By default it is set to false. When set to true, username and password will be prompted.

[-skip-config-validation <true>] - Skip the config validation

Use this parameter to skip the HTTP proxy configuration validation.

The proxy configuration is validated to verify that the specified server is reachable and is providing HTTP proxy service on the specified port.

The validation fails in the following cases:

- The server is not reachable.
- The specified port is invalid.
- HTTP proxy service is not configured on the specified server and port.
- Route or LIF does not exist.

Examples

The following example modifies the HTTP proxy server of the Vserver vs0 with Fully Qualified Domain Name as input for `-server` parameter:

```
cluster1::*> vserver http-proxy modify -vserver vs0 -server example.com
```

vserver http-proxy show

Display HTTP Proxy configuration

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

Description

The `vserver http-proxy show` command displays information about HTTP proxy configurations. The IPspace field is populated only if a Vserver is the system vserver of that IPspace. For all other Vservers, the IPspace field is empty.

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

Use this parameter to display information only about the HTTP proxy configuration of the Vservers you specify.

[-ipspace <text>] - Ipspace

Use this parameter to display information only about the HTTP proxy configuration of the IPspace you specify.

[-server <text>] - Proxy Server

Use this parameter to display information only about the HTTP proxy configurations that match the the Fully Qualified Domain Name or IP address you specify.

[-port <integer>] - Port

Use this parameter to display information only about the HTTP proxy configurations that match the port you specify.

[-is-auth-enabled {true|false}] - Authentication Enabled

Use this parameter to display information only about the HTTP proxy configurations that match the specified authentication enabled setting.

Examples

The following example displays information about all HTTP proxy configurations:

```
cluster1::*> vserver http-proxy show
Vserver         IPSpace        Server                                 Port
--------------- -------------- ---------------------------------
----------------
test            test           10.0.0.0                               3128
vs2             -              192.168.0.0                            3128
2 entries were displayed.
```

The following example displays information about all HTTP proxy configurations with `server` 10.0.0.0:

```
cluster1::*> vserver http-proxy show -server 10.0.0.0
Vserver         IPSpace        Server                                 Port
--------------- -------------- ---------------------------------
----------------
test            test           10.0.0.0                               3128
```

vserver iscsi commands

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 the following rules:

- Contains up to 128 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.

`[-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.

[-f, -force <true>] - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

Examples

```
cluster1::> vserver iscsi create -vserver vs_1
```

Creates the iSCSI service for Vserver 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.

> 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

```
cluster1::> vserver iscsi delete -vserver vs_1
```

Deletes the iSCSI service for Vserver vs_1.

Related Links

- 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 the following rules:

- Contains up to 128 bytes.
- Contains alphanumeric characters. The period ".", hyphen "-", and colon ":" are acceptable.
- Does not contain the underscore character "_".

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.

| `[-c, -clear <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.

`[-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
```

[-f, -force <true>] - Allow Non-Vendor Target Name (privilege: advanced)

Force the command to accept a target name that would normally be rejected as invalid.

Examples

```
cluster1::> vserver iscsi modify -vserver vs_1 -status-admin down
```

Modifies the status-admin of the iSCSI service for Vserver vs_1 to down.

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

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.

[-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

```
cluster1::> 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.

cluster1::> 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.

```
cluster1::*> 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.

```
cluster1::*> 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
RFC3720 DefaultTime2Retain Value (in sec): 20
            Login Phase Duration (in sec): 15
              Max Connections per Session: 4
                       Max I/O per Session: 128
  TCP Window Size all Sessions (in bytes): 131400
```

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

```
cluster1::> vserver iscsi start -vserver vs_1
```

Starts the iSCSI service for Vserver vs_1.

Related Links

- 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

```
cluster1::> vserver iscsi stop -vserver vs_1
```

Stops the iSCSI service for Vserver vs_1.

Related Links

- 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::> vserver iscsi command show -instance -vserver vs_1
server: vs_1
        Target Portal Group Name: tpgroup_1
               Target Session ID: 2
                      Command ID: 20797
                  Initiator Name: iqn.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-mrdsl <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-mrdsl <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 vs1
             Tpgroup              Conn  Local           Remote          TCP
Recv
Vserver      Name           TSIH  ID    Address         Address
Size
------------ ------------- ----- ----- --------------- ---------------
--------
vs1          vs1.iscsi          6     0 10.63.8.163     10.60.141.65
131400
vs1          vs1.iscsi          7     0 10.63.8.163     10.62.8.75
131400
2 entries were displayed.
```

Displays connection information on Vserver vs1.

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 (privilege: advanced)

Specifies the Vserver.

`-tpgroup <text>` - Target Portal Group (privilege: advanced)

Specifies the target portal group that contains the connection you want to shut down.

`-tsih <integer>` - Target Session ID (privilege: advanced)

Specifies the target session ID that you want to shut down.

`-connection-id <integer>` - Connection ID (privilege: advanced)

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.

Related Links

- 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>] - TPGroup 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
        Tpgroup       Initiator
Vserver Name     TSIH Name                   ISID              IGroup
------- -------- ---- -------------------- -----------------
-----------------
vs_1    vs_1.iscsi  6 iqn.1994-05.com.redhat:6ed6dfb0489e
                                            00:02:3d:03:00:00 -
vs_1    vs_1.iscsi  7 iqn.1993-08.org.debian:01:fa752b8a5a3a
                                            00:02:3d:01:00:00 igroup_1
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.

| -a, -all <true> - All }
Specifies that all logical interfaces on the Vserver are disabled.

[-f, -force <true>] - Force
When set to true, forces the termination of any active iSCSI sessions without prompting you for a confirmation.

Examples

```
cluster1::> 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.

| `-a, -all <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 modify

Modify network interfaces used for iSCSI connectivity

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

Description

The `vserver iscsi interface modify` command modifies the iSCSI specific configuration for an iSCSI LIF.

Parameters

`-vserver <Vserver Name>` - Vserver

Specifies the Vserver.

`-lif <lif-name>` - Logical Interface

Use this parameter to specify the logical interface on a Vserver that you want to modify.

[-sendtargets-fqdn <text>] - iSCSI Discovery SendTargets FQDN (privilege: advanced)

Use this parameter to specify the Fully Qualified Domain Name (FQDN) to return during an iSCSI Discovery SendTargets operation. To clear the FQDN, set this parameter to "". If unset, the IP address of the LIF is used in iSCSI SendTargets discovery. + This is not part of iSNS and will not affect the iSNS configuration.

Examples

The following example modifies the sendtargets-fqdn of the iSCSI LIF vs1_iscsi1 for Vserver vs1 to myhost.example.com.

```
cluster1::> vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1
-sendtargets_fqdn myhost.example.com
```

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>] - TPGroup Name

Use this parameter to display iSCSI logical interfaces that match the target portal group name that you specify.

[-t, -tpgroup-tag <integer>] - TPGroup 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 the 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.

[-sendtargets-fqdn <text>] - iSCSI Discovery SendTargets FQDN (privilege: advanced)

Use this parameter to display the iSCSI logical interfaces that match the iSCSI Discovery SendTargets Fully Qualified Domain Name (FQDN) that you specify.

Examples

The following example displays information for logical interfaces on Vserver vs_1.

```
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.
```

The following example displays the logical interface vs_1.iscsi with the relative target port ID of 1.

```
cluster1::> vserver iscsi interface show -vserver vs_1 -relative-port-id 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
```

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.

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.

| `-a, -all <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.

`[-f, -force <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.

Related Links

- 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.

| `-a, -all <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.

`[-f, -force <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 vs1
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 vs1.

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 and starts an iSNS service with the IP address of the iSNS server.

A Vserver management LIF must exist before you can create an iSNS service. This LIF is used to communicate with the iSNS server. To create a Vserver management LIF, use the network interface create command, with `-role` *data* and `-data-protocol` *none*.

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 vserver management LIF.

A default route must exist for the specified vserver. 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 vserver management LIF is not configured. When you set this option to "true," you create an iSNS service on a Vserver even if the vserver does not have a vserver management LIF.

Examples

```
cluster1::> 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.

```
cluster1::> 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.

Related Links

- network interface create

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

```
cluster1::> vserver iscsi isns delete -vserver vs_1
```

Deletes the iSNS service for Vserver vs_1.

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 vserver management LIF.

> A default route must exist for the specified vserver. 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 vserver management LIF is not configured. When you set this option to "true," you can modify the iSNS service on a Vserver even if the

vserver does not have a vserver management LIF.

Examples

```
cluster1::> iscsi isns modify -vserver vs_1 -status-admin up
```

Modifies the status-admin of the iSNS service for Vserver vs_1 to up.

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

```
cluster1::> 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.

```
cluster1::> 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

```
cluster1::> 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

```
cluster1::> 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

```
cluster1::> vserver iscsi isns update -vserver vs_1
```

Updates the iSNS server registration for Vserver vs_1.

vserver iscsi security add-initator-address-ranges

Add IP Address Ranges

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

Description

Add IP address ranges to an existing iSCSI security entry

Parameters

`-vserver <Vserver Name>` - Vserver
Specifies the Vserver.

`-i, -initiator-name <text>` - Initiator Name
Specifies the initiator.

`-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}` - Initiator IP Address Ranges
Specifies one or more initiator source IP address range. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
cluster1::> vserver iscsi security add-initator-address-range
-vserver vs1 -initiator-name iqn.1993-08.com.example:01:e3f87c7cf2e4
-initiator-address-range 192.168.2.1-192.168.2.255
```

Adds the IP address range 192.168.2.1-192.168.2.255 to initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 for vserver vs1.

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.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator that you want to create a security method for. You can use either an iqn such as iqn.1995-08.com.example:string or eui such as eui.0123456789abcdef for the initiator.

`-s, -auth-type {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.

`[-n, -user-name <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.

`[-m, -outbound-user-name <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.

`[-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}]` - Initiator IP Address Ranges

Specifies one or more initiator source IP address ranges. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
cluster1::> vserver iscsi security create -initiator
eui.0123456789abcdef -auth-type CHAP -user-name bob -outbound-user-name
bob2

Password: {enter password}

Outbound Password: {enter password}
```

Creates authentication method chap for initiator eui.0123456789abcdef with inbound and outbound usernames and passwords.

```
cluster1::> vserver iscsi security create -vserver vs_1
-initiator-name iqn.1995-08.com.example:e3f87c7cf2e4 -auth-type none
-initiator-address-ranges 192.168.1.1-192.168.1.255
```

Creates authentication method for initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 with IP address validation only.

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.

`-s, -auth-type {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.

[-n, -user-name <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.

{ [-m, -outbound-user-name <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::> vserver iscsi security default -vserver vs1 -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.

Related Links

- 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.

-i, -initiator-name <text> - Initiator Name

Specifies the initiator that you want to remove the authentication setting from.

Examples

```
cluster1::> vserver iscsi security delete -vserver vs1 -initiator
iqn.1992-08.com.example:abcdefg
```

Deletes initiator iqn.1992-08.com.example:abcdefg on Vserver vs1 from the authentication setting. The default authentication now applies to this initiator.

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.

`-i, -initiator-name <text>` - Initiator Name

Specifies the initiator name that you want to modify the existing authentication method.

`[-s, -auth-type {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.

`[-n, -user-name <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.

{ `[-m, -outbound-user-name <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.

Related Links

- vserver iscsi security delete

vserver iscsi security prepare-to-downgrade

Prepares the system for downgrade

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

Description

This command prepares the cluster for a downgrade to an earlier version of Data ONTAP. Before using this command verify that all security entries do not have any initiator address ranges defined. This may be done by running the command vserver iscsi security show *address-ranges*

Examples

```
cluster1::> vserver iscsi security prepare-to-downgrade
```

The above example will verify that the cluster is able to downgrade to a prior release of Data ONTAP.

Related Links

- vserver iscsi security show

vserver iscsi security remove-initator-address-ranges

Remove an IP Address Range

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

Description

Remove IP address ranges to an existing iSCSI security entry

Parameters

-vserver <Vserver Name> - Vserver

Specifies the Vserver.

-i, -initiator-name <text> - Initiator Name

Specifies the initiator.

-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>} - Initiator IP Address Ranges

Specifies one or more initiator source IP address range. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

Examples

```
netapp-clus-1::> vserver iscsi security remove-initator-address-range
-vserver vs1 -initiator-name iqn.1993-08.com.example:01:e3f87c7cf2e4
-initiator-address-range 192.168.2.1-192.168.2.255
```

Removes the IP address range 192.168.2.1-192.168.2.255 to the initiator iqn.1993-08.com.example:01:e3f87c7cf2e4 for vserver vs1.

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.

| [-address-masks]

Display the list of IP Address ranges in CIDR notation that each initiator is allowed to originate from. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

| [-address-ranges]

Display the list of IP Address ranges that each initiator is allowed to originate from. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address

and an end address. The start and end addresses themselves are included in the range.

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver

Use this parameter to display authentication information that matches the Vserver name that you specify.

[-i, -initiator-name <text>] - Initiator Name

Use this parameter to display authentication information that matches the initiator that you specify.

[-s, -auth-type {CHAP|deny|none}] - Authentication Type

Use this parameter to display authentication information that matches the authentication type that you specify.

[-n, -user-name <text>] - Inbound CHAP User Name

Use this parameter to display authentication information that matches the inbound CHAP user name that you specify.

[-m, -outbound-user-name <text>] - Outbound CHAP User Name

Use this parameter to display authentication information that matches the outbound CHAP user name that you specify.

[-auth-chap-policy <local>] - Authentication CHAP Policy

Use this parameter to display authentication information that matches the authentication CHAP policy that you specify.

[-initiator-address-ranges {<ipaddr>|<ipaddr>-<ipaddr>}] - Initiator IP Address Ranges

Use this parameter to display authentication information that matches the initiator address range that you specify. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range is: '192.168.1.100-192.168.1.150'.

An example of a valid IPv6 address range is: '2001:db8::1000:1-2001:db8::1000:50'.

[-initiator-address-masks <IP Address/Mask>,…] - Initiator IP Address Masks

Use this parameter to display authentication information that matches the initiator address masks that you specify. If this list is empty, the initiator is allowed to log in from any IP address. The IPv4 or IPv6 address range contains a start address and an end address. The start and end addresses themselves are included in the range.

An example of a valid IPv4 address range in CIDR notation is: 192.168.1.3/32.

An example of a valid IPv6 address range in CIDR notation is: 2001:db8::1000:1/128.

Examples

```
cluster1::> vserver iscsi security show -vserver vs1
                                  Auth   Auth CHAP Inbound CHAP  Outbound
CHAP
Vserver    Initiator Name         Type   Policy    User Name     User Name
---------- ---------------------- ------ --------- ------------
-------------
vs1       default                none   -         -             -
          iqn.2010-12.com.example:abcdefg
                                  CHAP   local     bob           bob2
2 entries were displayed.
```

Displays the authentication information for Vserver vs1.

```
cluster1::> vserver iscsi security show -address-ranges -vserver vs1

Vserver    Initiator Name         Initiator Address Ranges
---------- ----------------------
-----------------------------------------
vs1        iqn.2010-12.com.example:abcdefg
           iqn.2010-12.com.example:hijklmn
                                  192.168.1.100-192.168.1.150
                                  2001:db8::1000:1-2001:db8::1000:50

2 entries were displayed.
```

Displays the initiator and their valid address ranges for Vserver vs1.

```
cluster1::> vserver iscsi security show -address-masks -vserver vs1

Vserver    Initiator Name         Initiator Address Ranges
---------- ---------------------
-------------------------------------------
vs1        iqn.2010-12.com.example:abcdefg
     iqn.2010-12.com.example:hijklmn
          192.168.1.100/30
          192.168.1.104/29
          192.168.1.112/28
          192.168.1.128/28
          192.168.1.144/30
          192.168.1.148/31
          192.168.1.150/32
          2001:db8::1000:1/128
          2001:db8::1000:2/127
          2001:db8::1000:4/126
          2001:db8::1000:8/125
          2001:db8::1000:10/124
          2001:db8::1000:20/123
          2001:db8::1000:40/124
          2001:db8::1000:50/128
2 entries were displayed.
```

Displays the initiator and their valid address ranges for Vserver vs1.

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

```
cluster1::> vserver iscsi session show -vserver vs_1
          Tpgroup        Initiator                        Initiator
Vserver   Name    TSIH   Name                   ISID      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.
```

Related Links

- 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 (privilege: advanced)

Specifies the Vserver.

`-tpgroup <text>` - Target Portal Group (privilege: advanced)

Specifies the target portal group that contains the session you want to shutdown.

`-tsih <integer>` - Target Session ID (privilege: advanced)

Specifies the target session ID that you want to shut down.

Examples

```
cluster1::*> 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 .

Related Links

- 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-mrdsl <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-mrdsl <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
        Tpgroup      Max  Data PDU Data Seq Time 2 Time 2 Error   Imm
Initial
Vserver 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.

Related Links

- vserver iscsi modify

vserver locks commands

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 (privilege: advanced)

This parameter specifies the Vserver containing the lock.

-volume <volume name> - Volume (privilege: advanced)

This parameter specifies the name of the volume containing the lock.

[-lif <lif-name>] - Logical Interface (privilege: advanced)

This parameter specifies the logical interface through which the lock was established.

[-lif-id <integer>] - Logical Interface ID (privilege: advanced)

This parameter specifies the logical interface id through which the lock was established.

-path <text> - Object Path (privilege: advanced)

This parameter specifies a path to the lock.

| -lockid <UUID> - Lock UUID (privilege: advanced) }

This parameter specifies the universally unique identifier (UUID) for the lock. Queries and wildcard characters are not supported.

-owner-id <text> - Owner ID (privilege: advanced)

This parameter specifies an owner ID for a lock. This parameter must be used with the query notation { } exhibited in the second example.

-protocol <lock protocol> - Lock Protocol (privilege: advanced)

This parameter specifies the protocol that was used to establish a lock. This parameter must be used with the query notation { } exhibited in the second example.

-client-address <IP Address> - Client Address (privilege: advanced)

This parameter specifies a client address associated with a lock. This parameter must be used with the query notation { } exhibited in the second example.

-client-address-type {ipv4|ipv6|ipv6z} - Client Address Type (privilege: advanced)

This parameter specifies the type of ip address a client used to create its lock (ipv4, ipv6). This parameter must be used with the query notation { } exhibited in the second example.

-flexcache-volume <text> - FlexCache Volume Name (privilege: advanced)

This parameter specifies the name of the FlexCache volume. This parameter must be used with the query notation { } exhibited in the third example.

-flexcache-vserver <text> - FlexCache Vserver Name (privilege: advanced)

This parameter specifies the name of the Vserver hosting the FlexCache volume. This parameter must be used with the query notation { } exhibited in the third example.

-flexcache-cluster <text> - FlexCache Cluster Name (privilege: advanced)

This parameter specifies the name of the cluster hosting the FlexCache volume. This parameter must be used with the query notation { } exhibited in the third example.

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.
Do you want to continue? {y|n}: y
1 entry was acted on.
```

The vserver locks break command can also be issued using a query on the parameters available to the vserver locks show command. The following example breaks all NLM protocol lock objects locked by the client at address 12.34.56.78.

```
cluster1::*> vserver locks break { -protocol nlm -client-address
12.34.56.78 }
Warning: Breaking file locks can cause applications to become
unsynchronized
         and may lead to data corruption.
Do you want to continue? {y|n}: y
1 entry was acted on.
```

The following example breaks all FlexCache lock objects locked for FlexCache volume "fc1" in Vserver "vs12".

```
cluster1::*> vserver locks break { -flexcache-volume fc1 -flexcache
-vserver vs12 -flexcache-cluster cluster2 }
Warning: Breaking file locks can cause applications to become
unsynchronized
         and may lead to data corruption.
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

> The `vserver locks show` command is also used to display FlexCache specific locks. FlexCache locks are not stored on the FlexCache volume. Instead all of the locks are stored on the origin of a FlexCache volume. To view the FlexCache locks use the `vserver locks show` command on the origin 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.

| [-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.

For the FlexCache locks, this parameter displays the origin of a FlexCache volume name.

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

If you specify this parameter, the command displays information about locks established through the specified logical interface name.

For the FlexCache locks, this parameter is unset if the FlexCache volume is not local to the cluster.

[-lif-id <integer>] - Logical Interface ID (privilege: advanced)

If you specify this parameter, the command displays information about locks established through the specified logical interface id.

For the FlexCache locks, this parameter displays the logical interface id of the FlexCache cluster.

[-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).

[-is-constituent {true|false}] - Is Constituent Volume

If you specify this parameter, the command displays information only about volumes that either are or are not constituents of a FlexGroup, depending on the value provided.

[-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
- *fcache* : Delegations for 7-mode destination FlexCache volumes

[-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.
- *waiting* : The lock is waiting to be granted, because it conflicts with another lock.
- *denied* : The lock has been denied.
- *timeout* : 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.

[-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.

[-owner-id <text>] - Owner ID

If you specify this parameter, the command displays information only about locks with the specified owner ID. The owner ID is an opaque byte string generated by the server for each file lock request.

[-client-address <IP Address>] - Client Address

If you specify this parameter, the command displays information only about locks from the specified client IP address.

[-client-address-type {ipv4|ipv6|ipv6z}] - Client Address Type

If you specify this parameter, the command displays information only about locks corresponding to a certain IP address type. Please note that locks created over the NFSv4 or NFSv4.1 protocol cannot have their address types resolved. Valid options are:

- *ipv4* : Clients operating over an IPv4 interface.
- *ipv6* : Clients operating over an IPv6 interface.

[-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.

[-is-flexcache-lock {true|false}] - Is FlexCache Lock

If you specify this parameter, the command displays information only about locks with the specified value.

[-flexcache-volume <text>] - FlexCache Volume Name

If you specify this parameter, the command displays information only about locks with the specified FlexCache volume.

[-flexcache-vserver <text>] - FlexCache Vserver Name

If you specify this parameter, the command displays information only about locks with the specified Vserver hosting a FlexCache volume.

[-flexcache-vserver-uuid <UUID>] - FlexCache Vserver UUID

If you specify this parameter, the command displays information only about locks with the specified UUID of a Vserver hosting a FlexCache volume.

[-flexcache-volume-msid <integer>] - FlexCache Volume MSID

If you specify this parameter, the command displays information only about locks with the specified FlexCache volume MSID

[-flexcache-cluster <text>] - FlexCache Cluster Name

If you specify this parameter, the command displays information only about locks with the specified cluster hosting a FlexCache volume.

[-flexcache-lock-authority <text>] - FlexCache lock authority

If you specify this parameter, the command displays information only about locks with the specified authority granted to a FlexCache volume.

Examples

The following example displays default information about all locks:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path               LIF         Protocol  Lock Type
Client
-------- ------------------------- ----------- --------- -----------
----------
vol1     /vol1/notes.txt           node1_data1
                                                cifs      share-level
192.168.1.5
                Sharelock Mode: read_write-deny_delete
                                                          op-lock
192.168.1.5
                Oplock Level: read-batch
         /vol1/notes1.txt          node1_data1
                                                cifs      share-level
192.168.1.5
                Sharelock Mode: read_write-deny_delete
                                                          op-lock
192.168.1.5
                Oplock Level: batch
         /vol1                     node1_data2
                                                cifs      share-level
192.168.1.5
                Sharelock Mode: read-deny_delete
         /vol1/notes.txt           node1_data2
                                                cifs      share-level
192.168.1.5
                Sharelock Mode: read_write-deny_delete
                                                          op-lock
192.168.1.5
                Oplock Level: read-batch
7 entries were displayed.
```

The following example displays the SMB related information about all locks:

```
cluster1::> vserver locks show -smb-attrs

Vserver: vs0
Volume   Object Path               LIF         Protocol  Lock Type
Client
-------- ------------------------- ----------- --------- -----------
----------
vol1     /vol1/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
/vol1/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
/vol1                     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: -
/vol1/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: vol1
          Logical Interface: node1_data1
                Object Path: /vol1/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
        Client Address Type: ipv4
              SMB Open Type: durable
          SMB Connect State: connected
 SMB Expiration Time (Secs): -
          SMB Open Group ID:
625e2ff46ee5df1194ba0050569d37047058909c00000000873d2107000000004
Vserver: vs0
                    Volume: vol1
          Logical Interface: node1_data1
                Object Path: /vol1/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
        Client Address Type: ipv4
              SMB Open Type: -
          SMB Connect State: connected
 SMB Expiration Time (Secs): -
          SMB Open Group ID:
625e2ff46ee5df1194ba0050569d37047058909c00000000873d210700000000
Vserver: vs0
                     Volume: vol1
          Logical Interface: node1_data1
                Object Path: /vol1/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
        Client Address Type: ipv4
              SMB Open Type: durable
          SMB Connect State: connected
 SMB Expiration Time (Secs): -
          SMB Open Group ID:
625e2ff46ee5df1194ba0050569d370440fc8891000000005a3f210700000000
3 entries were displayed.
```

The following example displays the FlexCache locks:

```
cluster1::> vserver locks show

Vserver: vs34
Volume   Object Path               LIF         Protocol  Lock Type
Client
-------- ------------------------- ----------- --------- -----------
----------
origin   /origin/file1             data1       nlm       byte-range
10.235.224.139
                Bytelock Offset(Length): 0 (18446744073709551615)
         /origin/file3             data1       nlm       byte-range
10.234.133.121
                Bytelock Offset(Length): 0 (18446744073709551615)
                FlexCache Lock: true
         /origin/file2             -           nlm       byte-range
10.234.189.144
                Bytelock Offset(Length): 0 (18446744073709551615)
                FlexCache Lock: true
3 entries were displayed.
cluster1::> vserver locks show -fields flexcache-vserver, flexcache-
volume, flexcache-cluster

vserver volume lif   path          flexcache-volume flexcache-vserver
flexcache-cluster
------- ------ ----- ------------- ---------------- -----------------
-----------------
vs34    origin data1 /origin/file1 -                -                -
vs34    origin data1 /origin/file3 local_fc         vs34
cluster2
vs34    origin -     /origin/file2 fc1              vs12
cluster1
3 entries were displayed.
```

The following example displays default information about FlexCache and origin of FlexCache locks in list form:

```
cluster1::> vserver locks show -instance
Vserver: vs34
                    Volume: origin
         Logical Interface: data1
               Object Path: /origin/file1
                 Lock UUID: 173d10d6-f64c-4983-a2c2-9db0bc4f5c05
     Is Constituent Volume: false
             Lock Protocol: nlm
                 Lock Type: byte-range
   Node Holding Lock State: node1
```

```
                Lock State: granted
  Bytelock Starting Offset: 0
    Number of Bytes Locked: 18446744073709551615
     Bytelock is Mandatory: false
     Bytelock is Exclusive: false
     Bytelock is Superlock: false
          Bytelock is Soft: false
              Oplock Level: -
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
                  Owner ID: 31-
1134394073637370723034353236363630312e67646c2e656e676c61622e6e65746170
             Client Address: 10.235.224.139
       Client Address Type: ipv4
             SMB Open Type: -
         SMB Connect State: -
SMB Expiration Time (Secs): -
         SMB Open Group ID: -
         Is FlexCache Lock: -
     FlexCache Volume Name: -
    FlexCache Vserver Name: -
    FlexCache Vserver UUID: -
     FlexCache Volume MSID: -
    FlexCache Cluster Name: -
Vserver: vs34
                    Volume: origin
         Logical Interface: data1
               Object Path: /origin/file3
                 Lock UUID: e3bf0c78-7371-41b6-9eff-4fa81d64ca08
     Is Constituent Volume: false
             Lock Protocol: nlm
                 Lock Type: byte-range
   Node Holding Lock State: node1
                Lock State: granted
  Bytelock Starting Offset: 0
    Number of Bytes Locked: 18446744073709551615
     Bytelock is Mandatory: false
     Bytelock is Exclusive: false
     Bytelock is Superlock: false
          Bytelock is Soft: false
              Oplock Level: -
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
                  Owner ID: 25-113337407363737072303439343433331303031
```

```
            Client Address: 10.234.133.121
       Client Address Type: ipv4
             SMB Open Type: -
          SMB Connect State: -
SMB Expiration Time (Secs): -
         SMB Open Group ID: -
         Is FlexCache Lock: true
     FlexCache Volume Name: local_fc
    FlexCache Vserver Name: vs34
    FlexCache Vserver UUID: 388e3004-7520-11e8-8789-005056b47572
     FlexCache Volume MSID: 2160150696
    FlexCache Cluster Name: cluster2
Vserver: vs34
                    Volume: origin
         Logical Interface: -
               Object Path: /origin/file2
                 Lock UUID: c420b002-d78c-4157-94d5-55c186ef4df3
     Is Constituent Volume: false
             Lock Protocol: nlm
                 Lock Type: byte-range
   Node Holding Lock State: node1
               Lock State: granted
  Bytelock Starting Offset: 0
    Number of Bytes Locked: 18446744073709551615
     Bytelock is Mandatory: false
     Bytelock is Exclusive: false
     Bytelock is Superlock: false
          Bytelock is Soft: false
              Oplock Level: -
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
                  Owner ID: 32-113530407363737072303435323636343030 31
            Client Address: 10.234.189.144
       Client Address Type: ipv4
             SMB Open Type: -
          SMB Connect State: -
SMB Expiration Time (Secs): -
         SMB Open Group ID: -
         Is FlexCache Lock: true
     FlexCache Volume Name: fc1
    FlexCache Vserver Name: vs12
    FlexCache Vserver UUID: 5a943dd9-7520-11e8-b5e7-005056b47786
     FlexCache Volume MSID: 2150871844
    FlexCache Cluster Name: cluster1
3 entries were displayed.
```

vserver name-mapping commands

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 12500 name mappings in each direction.

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 {krb-unix|win-unix|unix-win} - 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.

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.

{ [-address <IP Address/Mask>] - IP Address with Subnet Mask

This optional parameter specifies the IP address that can be used to match the client's workstation IP address with the pattern.

| [-hostname <text>] - Hostname }

This optional parameter specifies the hostname that can be used to match the corresponding client's workstation IP address with the list of IP addresses with the pattern.

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 -address
10.238.33.245/24"
cluster1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 5 -pattern cifs -replacement "EXAMPLE\\Domain Users -hostname
google.com"
```

Related Links

- 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 {krb-unix|win-unix|unix-win} - 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 12500 name mappings in each direction.

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 {krb-unix|win-unix|unix-win} - 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.

{ [-address <IP Address/Mask>] - IP Address with Subnet Mask

This optional parameter specifies the IP address that can be used to match the client's workstation IP address with the pattern.

| [-hostname <text>] - Hostname }

This optional parameter specifies the hostname that can be used to match the corresponding client's workstation IP address with the list of IP addresses with the pattern.

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"
      cluster1::> vserver name-mapping insert -vserver vs1 -direction krb-
unix -position 3 -pattern
      "([^@/]+)(/[^@]+)?@SEC.EXAMPLE.COM" -replacement "\1 -address
10.238.33.245/24
```

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 12500 name mappings in each direction.

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 {krb-unix|win-unix|unix-win} - 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.

{ [-address <IP Address/Mask>] - IP Address with Subnet Mask

This optional parameter specifies the IP address that can be used to match the client's workstation IP address with the pattern.

| [-hostname <text>] - Hostname }

This optional parameter specifies the hostname that can be used to match the corresponding client's workstation IP address with the list of IP addresses with the pattern.

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\\(.+) -address 10.238.2.54/32"
cluster1::> vserver name-mapping modify -vserver vs1 -direction win-unix
-position 3 -pattern "EXAMPLE\\(.+) -hostname google.com"
```

vserver name-mapping refresh-hostname-ip

Refresh the IP addresses for configured hostnames

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

Description

The `vserver name-mapping refresh-hostname-ip` command will refresh the IP Address entries in the name-mapping configuration by resolving the hostname. If you run this command with no parameters, this will

refresh the IP address entries for every hostname in the name-mapping configuration.

Parameters

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

This parameter specifies the Vserver for which the hostname lookup needs to be done.

`[-direction {krb-unix|win-unix|unix-win}]` - Name Mapping Direction (privilege: advanced)

This optional parameter specifies the direction of the name-mapping entry for the hostname lookup.

`[-hostname <text>]` - Hostname (privilege: advanced)

This optional parameter specifies the hostname for which the lookup needs to be done.

Examples

```
cluster1::*> vserver name-mapping refresh-hostname-ip -vserver vs1
-direction win-unix -hostname
```

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 {krb-unix|win-unix|unix-win}] - 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.

[-address <IP Address/Mask>] - IP Address with Subnet Mask

If you specify this parameter, the command displays information only about the name mapping or mappings that use the specified IP address.

[-hostname <text>] - Hostname

If you specify this parameter, the command displays information only about the name mapping or mappings that use the specified hostname.

Examples

The following example displays information about all name mappings:

```
cluster1::> vserver name-mapping show
Vserver:   vs1
Direction: win-unix
Position Hostname          IP Address/Mask
-------- ----------------- -----------------
1        google.com        -                  Pattern:
EXAMPLE\\administrator
                                           Replacement: nobody
2        -                 10.238.2.34/32     Pattern: EXAMPLE\\(.+)
                                           Replacement: \_1
```

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 {krb-unix|win-unix|unix-win}` - 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 commands

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 parameter specifies the Vserver on which you want to create the NFS configuration.

[-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 `enabled`.

[-udp {enabled|disabled}] - UDP Protocol

This optional parameter specifies whether to enable NFS access over UDP. The default setting is `enabled`.

Even if UDP is disabled, if TCP is enabled, the Vserver does not block 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 disallow access for certain clients, including over UDP, you can use export-policy rules. 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`.

[-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`.

[-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 {fail|ignore|use-export-policy}] - 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` , this overrides the unix security options set in the relevant export rules. 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` at the time of creation.

[-chown-mode {restricted|unrestricted|use-export-policy}] - Vserver Change Ownership Mode (privilege: advanced)

This optional parameter specifies whether file ownership can be changed only by the superuser, or if a non-root user can also change file ownership. If you set this parameter to `restricted` , file ownership can be changed only by the superuser, even though the on-disk permissions allow a non-root user to change file ownership. If you set this parameter to `unrestricted` , file ownership can be changed by the superuser and by the non-root user, depending upon the access granted by on-disk permissions. If you set this parameter to `use-export-policy` , file ownership 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` .

[-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 (bytes) (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 (bytes) (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, and NFSv4.x protocols. The range is 8192 to 1048576. The default setting is 65536.

Setting the parameter value greater than 65536 may cause performance degradation for existing connections using smaller values. Contact technical support for guidance.

[-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` .

[-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` .

[-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` .

[-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` .

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.

[-v4-id-domain <nfs 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 defaultv4iddomain.com. However, the value of this parameter overrides the default. The domain name must be agreed upon by both the NFS client and the storage controller before NFSv4 operations can be executed. It is recommended that the domain be specified in the fully qualified domain name format.

[-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)

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 (and NTFS File Permissions in Unified Security Style)

This optional parameter specifies if the NFSv4 ACL is preserved or dropped when chmod is performed. In unified security style, this parameter also specifies if NTFS file permissions are preserved or dropped when chmod, chgrp, or chown are 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 or later clients. The default setting is `enabled` .

[-rquota {enabled|disabled}] - Rquota Enable

This optional parameter specifies whether to enable rquota over NFS. The default setting is `disabled` .

[-v4.1-implementation-domain <nfs domain>] - NFSv4.1 Implementation ID Domain (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later implementation domain.

[-v4.1-implementation-name <text>] - NFSv4.1 Implementation ID Name (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later implementation name.

[-v4.1-implementation-date <Date>] - NFSv4.1 Implementation ID Date (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later 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 or later. The default setting is `disabled` .

[-v4.1-referrals {enabled|disabled}] - NFSv4.1 Referral Support (privilege: advanced)

This optional parameter specifies whether Data ONTAP supports NFSv4.1 or later 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 or later referrals, set this option to `disabled` ; otherwise, those clients will not be able to access the file system.

[-v4.1-acl {enabled|disabled}] - NFSv4.1 ACL Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 or later 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` .

[-v4-numeric-ids {enabled|disabled}] - NFSv4 Support for Numeric Owner IDs

This optional parameter specifies whether the support for numeric string identifiers in NFSv4 owner attributes is enabled. The default setting is `enabled` .

[-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 or later read delegations. The

default setting is `disabled` .

[-v4.1-write-delegation {enabled|disabled}] - NFSv4.1 Write Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 or later write delegations. The default setting is `disabled` .

[-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` .

[-auth-sys-extended-groups {enabled|disabled}] - AUTH_SYS Extended Groups Enabled (privilege: advanced)

This optional parameter specifies whether Data ONTAP supports fetching auxillary groups from a name service rather than from the RPC header. The default setting is `disabled` .

[-extended-groups-limit <integer>] - AUTH_SYS and RPCSEC_GSS Auxillary Groups Limit (privilege: advanced)

This optional parameter specifies the maximum number of auxillary groups supported over RPC security flavors AUTH_SYS and RPCSEC_GSS in Data ONTAP. The range is 32 to 1024. The default value is 32.

[-validate-qtree-export {enabled|disabled}] - Validation of Qtree IDs for Qtree File Operations (privilege: advanced)

This optional parameter specifies whether clustered Data ONTAP performs an additional validation on qtree IDs. The default setting is `enabled` . This parameter is ignored unless a non-inherited policy has been or is assigned to a qtree.

[-mountd-port <integer>] - NFS Mount Daemon Port (privilege: advanced)

This optional parameter specifies which port the NFS mount daemon (mountd) uses. The port numbers allowed are 635 (the default) and 1024 through 9999.

[-nlm-port <integer>] - Network Lock Manager Port (privilege: advanced)

This optional parameter specifies which port the network lock manager (NLM) uses. The port numbers allowed are 1024 through 9999. The default setting is `4045` .

[-nsm-port <integer>] - Network Status Monitor Port (privilege: advanced)

This optional parameter specifies which port the network status monitor (NSM) uses. The port numbers allowed are 1024 through 9999. The default setting is `4046` .

[-rquotad-port <integer>] - NFS Quota Daemon Port (privilege: advanced)

This optional parameter specifies which port the NFS quota daemon (rquotad) uses. The port numbers allowed are 1024 through 9999. The default setting is `4049` .

[-permitted-enc-types <NFS Kerberos Encryption Type>,…] - Permitted Kerberos Encryption Types

This optional parameter specifies the permitted encryption types for Kerberos over NFS. The default setting is `des` ,`des3` ,`aes-128` ,`aes-256` .

[-showmount {enabled|disabled}] - Showmount Enabled

This optional parameter specifies whether to allow or disallow clients to see the Vserver's NFS exports list. The default setting is *`enabled`* .

Showmount leverages the MOUNT protocol in NFSv3 to issue an EXPORT query to the NFS server. If the mount port is not listening or blocked by a firewall, or if NFSv3 is disabled on the NFS server, showmount queries fail.

[-name-service-lookup-protocol {TCP|UDP}] - Set the Protocol Used for Name Services Lookups for Exports

This optional parameter specifies the protocol to use for doing name service lookups. The allowed values are `TCP` and `UDP` . The default setting is `UDP` .

[-map-unknown-uid-to-default-windows-user {enable|disable}] - Map Unknown UID to Default Windows User (privilege: advanced)

If you enable this optional parameter, unknown UNIX users that do not have a name mapping to a Windows user are mapped to the configured default Windows user. This allows all unknown UNIX users access with the credentials of the default Windows user. If you disable it, all unknown UNIX users without name mapping are always denied access. By default, this parameter is enabled.

[-netgroup-dns-domain-search {enabled|disabled}] - DNS Domain Search Enabled During Netgroup Lookup (privilege: advanced)

If you enable this optional parameter, during client access check evaluation in a netgroup, Data ONTAP performs an additional verification to ensure that the domain returned from DNS for that client is listed in the DNS configuration of the Vserver. This enables you to validate the domain when clients have the same short name in multiple domains. The default setting is *`enabled`* .

[-netgroup-trust-any-ns-switch-no-match {enabled|disabled}] - Trust No-Match Result from Any Name Service Switch Source During Netgroup Lookup (privilege: advanced)

This optional parameter specifies if you can consider a no-match result from any netgroup ns-switch source to be authoritative. If this option is enabled, then a no-match response from any one of the netgroup ns-switch sources is deemed conclusive even if other sources could not be searched. The default setting is 'disabled', which causes all netgroup ns-switch sources to be consulted before a no-match result is deemed

conclusive.

[-ntacl-display-permissive-perms {enabled|disabled}] - Display maximum NT ACL Permissions to NFS Client (privilege: advanced)

This optional parameter controls the permissions that are displayed to NFSv3 and NFSv4 clients on a file or directory that has an NT ACL set. When true, the displayed permissions are based on the maximum access granted by the NT ACL to any user. When false, the displayed permissions are based on the minimum access granted by the NT ACL to any user. The default setting is *false* .

[-v3-ms-dos-client {enabled|disabled}] - NFSv3 MS-DOS Client Support

This optional parameter specifies whether to enable access for NFSv3 MS-DOS clients. The default setting is *disabled* .

[-ignore-nt-acl-for-root {enabled|disabled}] - Ignore the NT ACL Check for NFS User 'root' (privilege: advanced)

This optional parameter specifies whether Windows ACLs affect root access from NFS. If this option is enabled, root access from NFS ignores the NT ACL set on the file or directory. If auditing is enabled for the Vserver and there is no name-mapping present, then a default SMB credential (Builtin\administrator) is used for auditing, and an EMS warning is generated. The default setting is 'disabled', which causes NFS 'root' to be mapped to a Windows account, like any other NFS user.

[-cached-cred-positive-ttl <integer>] - Time To Live Value (in msecs) of a Positive Cached Credential (privilege: advanced)

This optional parameter specifies the age of the positive cached credentials after which they will be cleared from the cache. The value specified must be between 60000 and 604800000. The default setting is `86400000` .

[-cached-cred-negative-ttl <integer>] - Time To Live Value (in msecs) of a Negative Cached Credential (privilege: advanced)

This optional parameter specifies the age of the negative cached credentials after which they will be cleared from the cache. The value specified must be between 60000 and 604800000. The default setting is `7200000` .

[-skip-root-owner-write-perm-check {enabled|disabled}] - Skip Permission Check for NFS Write Calls from Root/Owner (privilege: advanced)

This optional parameter specifies if permission checks are to be skipped for NFS WRITE calls from root/owner. For copying read-only files to a destination folder which has inheritable ACLs, this option must be *enabled* . Warning: When *enabled* , if an NFS client does not make use of an NFS ACCESS call to check for user-level permissions and then tries to write onto read-only files, the operation will succeed. The default setting is *disabled* .

[-v3-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv3 FSIDs and File IDs (privilege: advanced)

This optional parameter specifies whether Data ONTAP uses 64 bits (instead of 32 bits) for file system identifiers (FSIDs) and file identifiers (file IDs) that are returned to NFSv3 clients. The default setting is *disabled* . When `-v3-fsid-change` is disabled, enable this parameter to avoid file ID collisions.

[-v4-inherited-acl-preserve {enabled|disabled}] - Ignore Client Specified Mode Bits and Preserve Inherited NFSv4 ACL When Creating New Files or Directories (privilege: advanced)

This optional parameter specifies whether the client-specified mode bits should be ignored and the inherited NFSv4 ACL should be preserved when creating new files or directories. The default setting is *disabled* .

[-v3-search-unconverted-filename {enabled|disabled}] - Fallback to Unconverted Filename Search (privilege: advanced)

This optional parameter specifies whether to continue search without converting the filename to the Unicode character set while doing lookup in a directory.

[-file-session-io-grouping-count <integer>] - I/O Count to Be Grouped as a Session (privilege: advanced)

This optional parameter specifies the number of read or write operations on a file from a single client that are grouped and considered as one session for event generation applications, such as FPolicy. The event is generated on the first read or write of a file, and subsequently the event is generated only after the specified `-file-session-io-grouping-count` . The default value is *5000* .

[-file-session-io-grouping-duration <integer>] - Duration for I/O to Be Grouped as a Session (Secs) (privilege: advanced)

This optional parameter specifies the duration for which the read or write operationss on a file from a single client are grouped and considered as one session for event generation applications, such as FPolicy. The default value is *120* seconds.

[-checksum-for-replay-cache {enabled|disabled}] - Enable or disable Checksum for Replay-Cache (privilege: advanced)

This optional parameter specifies whether to enable replay cache checksum for NFS requests . The default value is *enabled* .

[-cached-cred-harvest-timeout <integer>] - Harvest timeout (in msecs) for a Cached Credential (privilege: advanced)

This optional parameter specifies the harvest timeout for cached credentials. The value specified must be between 60000 and 604800000. The default setting is `86400000` .

[-idle-connection-timeout <integer>] - Idle Connection Timeout Value (in seconds)

This optional parameter specifies the idle connection timeout value for NFS connections in seconds. The value specified must be between 120 and 86400.

[-allow-idle-connection {enabled|disabled}] - Are Idle NFS Connections Supported

This optional parameter specifies whether to enable idle NFS connections. The default setting is `disabled` .

[-v3-hide-snapshot {enabled|disabled}] - Hide Snapshot Directory under NFSv3 Mount Point

This optional parameter specifies whether to hide the .snapshot directory while listing under NFSv3 mount points. However an explicit access to the .snapshot directory will still be allowed even though the option is enabled. The default setting is `disabled` .

[-showmount-rootonly {enabled|disabled}] - Provide Root Path as Showmount State

This optional parameter specifies whether to provide root path as showmount state when `-showmount` parameter is disabled. The default value for `showmount-rootonly` is *disabled* .

[-v4-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv4.x FSIDs and File IDs (privilege: advanced)

This optional parameter specifies whether Data ONTAP uses 64 bits (instead of 32 bits) for file system identifiers (FSIDs) and file identifiers (file IDs) that are returned to NFSv4.x clients. The default setting is *enabled* . When `-v4-fsid-change` is disabled, enable this parameter to avoid file ID collisions.

[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support (privilege: advanced)

This optional parameter specifies whether to enable security labels for NFSv4.2. 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
```

Related Links

- 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.

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.

`[-udp {enabled|disabled}]` - UDP Protocol

This optional parameter specifies whether to enable NFS access over UDP.

Even if UDP is disabled, if TCP is enabled, the Vserver does not block 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 disallow access for certain clients, including over UDP, you can use export-policy rules. 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.

`[-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 {fail|ignore|use-export-policy}] - 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` , this overrides the unix security options set in the relevant export rules. 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` at the time of creation.

[-chown-mode {restricted|unrestricted|use-export-policy}] - Vserver Change Ownership Mode (privilege: advanced)

This optional parameter specifies whether file ownership can be changed only by the superuser, or if a non-root user can also change file ownership. If you set this parameter to `restricted` , file ownership can be changed only by the superuser, even though the on-disk permissions allow a non-root user to change file ownership. If you set this parameter to `unrestricted` , file ownership can be changed by the superuser and by the non-root user, depending upon the access granted by on-disk permissions. If you set this parameter to `use-export-policy` , file ownership 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 (bytes) (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 (bytes) (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 and NFSv4.x protocols. The range is 8192 to 1048576.

The default setting is 65536 when created. Warning: Increasing/decreasing the value of this parameter could affect the performance for existing connections.

[-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.

[-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.

[-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.

[-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.

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.

[-v4-id-domain <nfs 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 defaultv4iddomain.com. However, the value of this parameter overrides the default. The domain name must be agreed upon by both the NFS client and the storage controller before NFSv4 operations can be executed. It is recommended that the domain be specified in the fully qualified domain name format.

[-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)

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 (and NTFS File Permissions in Unified Security Style)

This optional parameter specifies if the NFSv4 ACL is preserved or dropped when chmod is performed. In unified security style, this parameter also specifies if NTFS file permissions are preserved or dropped when chmod, chgrp, or chown are 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 or later 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.

[-v4.1-implementation-domain <nfs domain>] - NFSv4.1 Implementation ID Domain (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later implementation domain.

[-v4.1-implementation-name <text>] - NFSv4.1 Implementation ID Name (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later implementation name.

[-v4.1-implementation-date <Date>] - NFSv4.1 Implementation ID Date (privilege: advanced)

This optional parameter specifies the NFSv4.1 or later 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 or later. The default setting is `disabled` 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 or later 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 or later referrals, set this option to `disabled` ; otherwise, those clients will not be able to access the file system.

[-v4.1-acl {enabled|disabled}] - NFSv4.1 ACL Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 or later 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.

[-v4-numeric-ids {enabled|disabled}] - NFSv4 Support for Numeric Owner IDs

This optional parameter specifies whether to enable the support for numeric string identifiers in NFSv4 owner attributes. The default setting is `enabled` at the time of creation.

[-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 or later read delegations. The default setting is `disabled` when created.

[-v4.1-write-delegation {enabled|disabled}] - NFSv4.1 Write Delegation Support

This optional parameter specifies whether Data ONTAP supports NFSv4.1 or later write delegations. The default setting is `disabled` when created.

[-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` .

[-auth-sys-extended-groups {enabled|disabled}] - AUTH_SYS Extended Groups Enabled (privilege: advanced)

This optional parameter specifies whether Data ONTAP supports fetching auxillary groups from a name service rather than from the RPC header. The default setting is `disabled` .

[-extended-groups-limit <integer>] - AUTH_SYS and RPCSEC_GSS Auxillary Groups Limit (privilege: advanced)

This optional parameter specifies the maximum number of auxillary groups supported over RPC security flavors AUTH_SYS and RPCSEC_GSS in Data ONTAP. The range is 32 to 1024. The default value is 32.

[-validate-qtree-export {enabled|disabled}] - Validation of Qtree IDs for Qtree File Operations (privilege: advanced)

This optional parameter specifies whether clustered Data ONTAP performs an additional validation on qtree IDs. The default setting is `enabled` . This parameter is ignored unless a non-inherited policy has been or is assigned to a qtree.

[-mountd-port <integer>] - NFS Mount Daemon Port (privilege: advanced)

This optional parameter specifies which port the NFS mount daemon (mountd) uses. The port numbers allowed are 635 (the default) and 1024 through 9999.

[-nlm-port <integer>] - Network Lock Manager Port (privilege: advanced)

This optional parameter specifies which port the network lock manager (NLM) uses. The port numbers allowed are 1024 through 9999. The default setting is `4045` .

[-nsm-port <integer>] - Network Status Monitor Port (privilege: advanced)

This optional parameter specifies which port the network status monitor (NSM) uses. The port numbers allowed are 1024 through 9999. The default setting is `4046` .

[-rquotad-port <integer>] - NFS Quota Daemon Port (privilege: advanced)

This optional parameter specifies which port the NFS quota daemon (rquotad) uses. The port numbers allowed are 1024 through 9999. The default setting is `4049` .

[-permitted-enc-types <NFS Kerberos Encryption Type>,…] - Permitted Kerberos Encryption Types

This optional parameter specifies the permitted encryption types for Kerberos over NFS. The default setting is `des` ,`des3` ,`aes-128` ,`aes-256` .

[-showmount {enabled|disabled}] - Showmount Enabled

This optional parameter specifies whether to allow or disallow clients to see the Vserver's NFS exports list. The default setting is *`enabled`* .

> Showmount leverages the MOUNT protocol in NFSv3 to issue an EXPORT query to the NFS server. If the mount port is not listening or blocked by a firewall, or if NFSv3 is disabled on the NFS server, showmount queries fail.

[-name-service-lookup-protocol {TCP|UDP}] - Set the Protocol Used for Name Services Lookups for Exports

This optional parameter specifies the protocol to use for doing name service lookups. The allowed values are `TCP` and `UDP` . The default setting is `UDP` .

[-map-unknown-uid-to-default-windows-user {enable|disable}] - Map Unknown UID to Default Windows User (privilege: advanced)

If you enable this optional parameter, unknown UNIX users that do not have a name mapping to a Windows user are mapped to the configured default Windows user. This allows all unknown UNIX users access with the credentials of the default Windows user. If you disable it, all unknown UNIX users without name mapping are always denied access. By default, this parameter is enabled.

[-netgroup-dns-domain-search {enabled|disabled}] - DNS Domain Search Enabled During Netgroup Lookup (privilege: advanced)

If you enable this optional parameter, during client access check evaluation in a netgroup, Data ONTAP performs an additional verification to ensure that the domain returned from DNS for that client is listed in the DNS configuration of the Vserver. This enables you to validate the domain when clients have the same short name in multiple domains. The default setting is *`enabled`* .

[-netgroup-trust-any-ns-switch-no-match {enabled|disabled}] - Trust No-Match Result from Any Name Service Switch Source During Netgroup Lookup (privilege: advanced)

This optional parameter specifies if you can consider a no-match result from any of the netgroup ns-switch sources to be authoritative. If this option is enabled, then a no-match response from any of the netgroup ns-switch sources is deemed conclusive even if other sources could not be searched. The default setting is 'disabled', which causes all netgroup ns-switch sources to be consulted before a no-match result is deemed conclusive.

[-ntacl-display-permissive-perms {enabled|disabled}] - Display maximum NT ACL Permissions to NFS Client (privilege: advanced)

This optional parameter controls the permissions that are displayed to NFSv3 and NFSv4 clients on a file or directory that has an NT ACL set. When true, the displayed permissions are based on the maximum access granted by the NT ACL to any user. When false, the displayed permissions are based on the minimum access granted by the NT ACL to any user. The default setting is *false* .

[-v3-ms-dos-client {enabled|disabled}] - NFSv3 MS-DOS Client Support

This optional parameter specifies whether to enable access for NFSv3 MS-DOS clients. The default setting is *disabled* at the time of creation.

[-ignore-nt-acl-for-root {enabled|disabled}] - Ignore the NT ACL Check for NFS User 'root' (privilege: advanced)

This optional parameter specifies whether Windows ACLs affect root access from NFS. If this option is enabled, root access from NFS ignores the NT ACL set on the file or directory. If auditing is enabled for the Vserver and there is no name-mapping present, then a default SMB credential (Builtin\administrator) is used for auditing, and an EMS warning is generated. The default setting is 'disabled', which causes NFS 'root' to be mapped to a Windows account, like any other NFS user.

[-cached-cred-positive-ttl <integer>] - Time To Live Value (in msecs) of a Positive Cached Credential (privilege: advanced)

This optional parameter specifies the age of the positive cached credentials after which they will be cleared from the cache. The value specified must be between 60000 and 604800000. The default setting is `86400000` .

[-cached-cred-negative-ttl <integer>] - Time To Live Value (in msecs) of a Negative Cached Credential (privilege: advanced)

This optional parameter specifies the age of the negative cached credentials after which they will be cleared from the cache. The value specified must be between 60000 and 604800000. The default setting is `7200000` .

[-skip-root-owner-write-perm-check {enabled|disabled}] - Skip Permission Check for NFS Write Calls from Root/Owner (privilege: advanced)

This optional parameter specifies if permission checks are to be skipped for NFS WRITE calls from root/owner. For copying read-only files to a destination folder which has inheritable ACLs, this option must be *enabled* . Warning: When *enabled* , if an NFS client does not make use of an NFS ACCESS call to check for user-level permissions and then tries to write onto read-only files, the operation will succeed. The default setting is *disabled* .

[-v3-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv3 FSIDs and File IDs (privilege: advanced)

This optional parameter specifies whether Data ONTAP uses 64 bits (instead of 32 bits) for file system identifiers (FSIDs) and file identifiers (file IDs) that are returned to NFSv3 clients. If you change the value of this parameter, clients must remount any paths over which they are using NFSv3. When `-v3-fsid`

`-change` is disabled, enable this parameter to avoid file ID collisions.

[-v4-inherited-acl-preserve {enabled|disabled}] - Ignore Client Specified Mode Bits and Preserve Inherited NFSv4 ACL When Creating New Files or Directories (privilege: advanced)

This optional parameter specifies whether the client-specified mode bits should be ignored and the inherited NFSv4 ACL should be preserved when creating new files or directories. The default setting is *disabled*.

[-v3-search-unconverted-filename {enabled|disabled}] - Fallback to Unconverted Filename Search (privilege: advanced)

This optional parameter specifies whether to continue search without converting the filename to the Unicode character set while doing lookup in a directory.

[-file-session-io-grouping-count <integer>] - I/O Count to Be Grouped as a Session (privilege: advanced)

This optional parameter specifies the number of read or write operations on a file from a single client that are grouped and considered as one session for event generation applications, such as FPolicy. The event is generated on the first read or write of a file, and subsequently the event is generated only after the specified `-file-session-io-grouping-count`. The default value is *5000*.

[-file-session-io-grouping-duration <integer>] - Duration for I/O to Be Grouped as a Session (Secs) (privilege: advanced)

This optional parameter specifies the duration for which the read or write operationss on a file from a single client are grouped and considered as one session for event generation applications, such as FPolicy. The default value is *120* seconds.

[-checksum-for-replay-cache {enabled|disabled}] - Enable or disable Checksum for Replay-Cache (privilege: advanced)

This optional parameter specifies whether to enable replay cache checksum for NFS requests. The default value is *enabled*.

[-cached-cred-harvest-timeout <integer>] - Harvest timeout (in msecs) for a Cached Credential (privilege: advanced)

This optional parameter specifies the harvest timeout for cached credentials. The value specified must be between 60000 and 604800000. The default setting is `86400000`.

[-idle-connection-timeout <integer>] - Idle Connection Timeout Value (in seconds)

This optional parameter specifies the idle connection timeout for NFS connections. The value specified must be between 120 and 86400.

[-allow-idle-connection {enabled|disabled}] - Are Idle NFS Connections Supported

This optional parameter specifies whether to enable idle NFS connections. The default setting is `disabled`.

[-v3-hide-snapshot {enabled|disabled}] - Hide Snapshot Directory under NFSv3 Mount Point

This optional parameter specifies whether to hide the .snapshot directory while listing under NFSv3 mount points. However an explicit access to the .snapshot directory will still be allowed even though the option is enabled. The default setting is `disabled` at the time of creation.

[-showmount-rootonly {enabled|disabled}] - Provide Root Path as Showmount State

This optional parameter specifies whether to provide root path as showmount state when `-showmount` parameter is disabled. The default value for `showmount-rootonly` is *disabled*.

[-v4-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv4.x FSIDs and File IDs (privilege: advanced)

This optional parameter specifies whether Data ONTAP uses 64 bits (instead of 32 bits) for file system identifiers (FSIDs) and file identifiers (file IDs) that are returned to NFSv4.x clients. If you change the value of this parameter, clients must remount any paths over which they are using NFSv4.x. When `-v4-fsid-change` is disabled, enable this parameter to avoid file ID collisions.

[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support (privilege: advanced)

This optional parameter specifies whether to enable security labels for NFSv4.2. The default setting is `disabled` at the time of creation.

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
```

Related Links

- 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 prepare-for-v3-ms-dos-client-downgrade

(DEPRECATED)-Disable NFSv3 MS-DOS Client Support

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

Description

This command is deprecated and may be removed in a future release.

The `vserver nfs prepare-for-v3-ms-dos-client-downgrade` command verifies that the NFSv3 MS-DOS client setting is disabled on all Vservers and disables the NFSv3 MS-DOS client support capability on the cluster when downgrading Data ONTAP to a version that does not support NFSv3 MS-DOS clients.

Examples

The following example disables NFSv3 MS-DOS client support on the Vservers.

```
cluster::1> vserver nfs prepare-for-v3-ms-dos-client-downgrade
```

vserver nfs prepare-to-downgrade

Remove NFS configurations that are not compatible with earlier versions of Data ONTAP

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

Description

The `vserver nfs prepare-to-downgrade` command removes NFS configurations incompatible with the earlier release of Data ONTAP.

Parameters

-disable-feature-set <downgrade version> - Data ONTAP Version (privilege: advanced)

This parameter specifies the Data ONTAP version that introduced the new NFS configurations and needs to be removed before downgrade. The value can be one of the following:

- 9.2.0 - Remove the NFS configurations introduced in Data ONTAP release 9.2.0. The configurations include the following:
- `-file-session-io-grouping-count` .
- `-file-session-io-grouping duration` .

Examples

```
cluster1::*> vserver nfs prepare-to-downgrade -disable-feature-set 9.2.0
```

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. + + All NFSv4.1 options apply to NFSv4.1 or later versions.

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 the `v3` option matches the specified input.

[-v4.0 {enabled|disabled}] - NFS v4.0

If you specify this parameter, the command displays information only about NFS-enabled Vservers for which the `v4.0` option matches the specified input.

[-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.

[-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 the `enable-ejukebox` option matches the specified input.

[-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 the `v3-connection-drop` option matches the specified input.

[-ntfs-unix-security-ops {fail|ignore|use-export-policy}] - 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 matches the specified input.

[-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 the chown-mode setting matches the specified input.

[-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 the `trace-enabled` option matches the specified input.

[-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 (bytes) (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 (bytes) (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 1048576.

[-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 the `v4.0-acl` option matches the specified input.

[-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 the `v4.0-read-delegation` option matches the specified input.

[-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 the `v4.0-write-delegation` option matches the specified input.

[-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 the `v4.0-referrals` option matches the specified input.

[-v4-id-domain <nfs domain>] - NFSv4 ID Mapping Domain

If you specify this parameter, the command displays information only about the NFS-enabled Vservers having the specified domain name.

[-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)

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 (and NTFS File Permissions in Unified Security Style)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `v4-acl-preserve` option matches the specified input.

[-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 the `v4.1` option matches the specified input.

[-rquota {enabled|disabled}] - Rquota Enable

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `rquota` option matches the specified input.

[-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 the `v4.1-implementation-domain` option matches the specified input.

[-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 the `v4.1-implementation-name` option matches the specified input.

[-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 the `v4.1-implementation-date` option matches the specified input.

[-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 the `v4.1-pnfs` option matches the specified input.

[-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 the `v4.1-referrals` option matches the specified input.

[-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 the `v4.1-acl` option matches the specified input.

[-vstorage {enabled|disabled}] - NFS vStorage Support

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `vstorage` option matches the specified input.

[-v4-numeric-ids {enabled|disabled}] - NFSv4 Support for Numeric Owner IDs

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `v4-numeric-ids` option matches the specified input.

[-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 the `v4.1-read-delegation` option matches the specified input.

[-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 the `v4.1-write-delegation` option matches the specified input.

[-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 information only about the NFS-enabled Vservers for which the `v4.x-session-num-slots` option matches the specified input. 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 information only about the NFS-enabled Vservers for which the `v4.x-session-slot-reply-cache-size` option matches the specified input. 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 displays information only about the NFS-enabled Vservers for which the `v4-acl-max-aces` option matches the specified input.

[-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 the `mount-rootonly` option matches the specified input.

[-nfs-rootonly {enabled|disabled}] - NFS Root Only

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `nfs-rootonly` option matches the specified input.

[-auth-sys-extended-groups {enabled|disabled}] - AUTH_SYS Extended Groups Enabled (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `auth-sys-extended-groups` option matches the specified input.

[-extended-groups-limit <integer>] - AUTH_SYS and RPCSEC_GSS Auxillary Groups Limit (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers for which the `extended-groups-limit` option matches the specified input. The range is 32 to 1024.

[-validate-qtree-export {enabled|disabled}] - Validation of Qtree IDs for Qtree File Operations (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `validate-qtree-export` option matches the specified input.

[-mountd-port <integer>] - NFS Mount Daemon Port (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `mountd-port` option matches the specified input.

[-nlm-port <integer>] - Network Lock Manager Port (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `nlm-port` option matches the specified input.

[-nsm-port <integer>] - Network Status Monitor Port (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `nsm-port` option matches the specified input.

[-rquotad-port <integer>] - NFS Quota Daemon Port (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `rquotad-port` option matches the specified input.

[-permitted-enc-types <NFS Kerberos Encryption Type>,…] - Permitted Kerberos Encryption Types

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `permitted-enc-types` option matches any of the following : des, des3, aes-128, aes-256.

[-showmount {enabled|disabled}] - Showmount Enabled

If you specify this parameter, the command displays information only about the NFS-enabled Vserver's for which the `showmount` option matches the specified input.

[-name-service-lookup-protocol {TCP|UDP}] - Set the Protocol Used for Name Services Lookups for Exports

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-name-service-lookup-protocol` matches the parameter.

[-map-unknown-uid-to-default-windows-user {enable|disable}] - Map Unknown UID to Default Windows User (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-map-unknown-uid-to-default-windows-user` is enabled or disabled.

[-netgroup-dns-domain-search {enabled|disabled}] - DNS Domain Search Enabled During Netgroup Lookup (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-netgroup-dns-domain-search` is enabled or disabled.

[-netgroup-trust-any-ns-switch-no-match {enabled|disabled}] - Trust No-Match Result from Any Name Service Switch Source During Netgroup Lookup (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-netgroup-trust-any-ns-switch-no-match` is enabled or disabled.

[-ntacl-display-permissive-perms {enabled|disabled}] - Display maximum NT ACL Permissions to NFS Client (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-ntacl-display-permissive-perms` matches the parameter.

[-v3-ms-dos-client {enabled|disabled}] - NFSv3 MS-DOS Client Support

If you specify this parameter, the command displays information only about NFS-enabled Vservers for which NFSv3 MS-DOS client support is enabled or disabled.

[-ignore-nt-acl-for-root {enabled|disabled}] - Ignore the NT ACL Check for NFS User 'root' (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-ignore-nt-acl-for-root` is enabled or disabled.

[-cached-cred-positive-ttl <integer>] - Time To Live Value (in msecs) of a Positive Cached Credential (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers time to live value of the positive cached credentials.

[-cached-cred-negative-ttl <integer>] - Time To Live Value (in msecs) of a Negative Cached Credential (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers time to

live value of the negative cached credentials.

[-skip-root-owner-write-perm-check {enabled|disabled}] - Skip Permission Check for NFS Write Calls from Root/Owner (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-skip-root-owner-write-perm-check` is enabled or disabled.

[-v3-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv3 FSIDs and File IDs (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-v3-64bit-identifiers` is enabled or disabled.

[-v4-inherited-acl-preserve {enabled|disabled}] - Ignore Client Specified Mode Bits and Preserve Inherited NFSv4 ACL When Creating New Files or Directories (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers for which `-v4-inherited-acl-preserve` matches the specified input.

[-v3-search-unconverted-filename {enabled|disabled}] - Fallback to Unconverted Filename Search (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers for which `-v3-search-unconverted-filename` matches the specified input.

[-file-session-io-grouping-count <integer>] - I/O Count to Be Grouped as a Session (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled SVMs for which the `-file-session-io-grouping-count` matches the specified input.

[-file-session-io-grouping-duration <integer>] - Duration for I/O to Be Grouped as a Session (Secs) (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled SVMs for which the `-file-session-io-grouping-duration` matches the specified input.

[-checksum-for-replay-cache {enabled|disabled}] - Enable or disable Checksum for Replay-Cache (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled SVMs for which the `-checksum-for-replay-cache` matches the specified input.

[-cached-cred-harvest-timeout <integer>] - Harvest timeout (in msecs) for a Cached Credential (privilege: advanced)

If you specify this parameter, the command displays information about the NFS-enabled Vservers harvest timeout for cached credentials.

[-idle-connection-timeout <integer>] - Idle Connection Timeout Value (in seconds)

If you specify this parameter, the command displays information about the NFS-enabled Vservers idle connections timeout

[-allow-idle-connection {enabled|disabled}] - Are Idle NFS Connections Supported

If you specify this parameter, the command displays information only about NFS-enabled Vservers for which the `-allow-idle-connection` option matches the specified input.

[-v3-hide-snapshot {enabled|disabled}] - Hide Snapshot Directory under NFSv3 Mount Point

If you specify this parameter, the command displays information about the NFS-enabled Vservers for which `-v3-hide-snapshot` matches the specified input.

[-showmount-rootonly {enabled|disabled}] - Provide Root Path as Showmount State

If you specify this parameter, the command displays information about the NFS-enabled Vservers for which `-showmount-rootonly` matches the specified input.

[-v4-64bit-identifiers {enabled|disabled}] - Use 64 Bits for NFSv4.x FSIDs and File IDs (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which `-v4-64bit-identifiers` is enabled or disabled.

[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support (privilege: advanced)

If you specify this parameter, the command displays information only about the NFS-enabled Vservers for which the `v4.2-seclabel` option matches the specified input.

Examples

The following example displays information about all NFS-enabled Vservers:

```
cluster1::> vserver nfs show
       General                                              Default
Vserver      Access  v3       v4       v4.1     UDP      TCP      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:

```
cluster1::*> 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 connected-clients show

Display List of recent NFS clients information

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

Description

The `nfs connected-clients show ` command displays information about currently connected NFS clients, other NFS clients that are are currently idle but can be connected, and a list of recently unmounted clients.

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 Name

Use this parameter to display information only about the specified node.

`[-vserver <vserver>]` - Vserver

Use this parameter to display information only about the specified vserver.

`[-data-lif-ip <IP Address>]` - Data LIF IP Address

Use this parameter to display information only about the specified data LIF IP.

`[-client-ip <IP Address>]` - Client IP Address

Use this parameter to display information only about the specified client IP.

[-volume <volume name>] - Volume Accessed

Use this parameter to display information only about the specified volume.

[-protocol <Client Access Protocol>] - Protocol Version

Use this parameter to display information only about the specified protocol.

[-idle-time <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Idle Time (Sec)

Use this parameter to display the time elapsed since the client sent the last request for this volume.

[-local-reqs <integer>] - Number of Local Reqs

Use this parameter to display a counter tracking requests that are sent to the volume with fast-path.

[-remote-reqs <integer>] - Number of Remote Reqs

Use this parameter to display a counter tracking requests that are sent to the volume with slow-path to remote Dblade using a CSM session.

[-policy-name <text>] - Export Policy Name

Use this parameter to display the Policy Name for this volume.

Examples

The following example displays the connected clients information.

```
cluster-1::*> nfs connected-clients show
Node: vsim1
  Vserver: vs1
  Data-Ip: 10.140.72.214
Client-Ip      Protocol Volume    Policy   Idle-Time    Local-Reqs Remote-
Reqs
-------------- -------- --------- -------- ------------ ----------
----------
10.140.137.57  nfs4     rvol1     pol1     5s           9          0
10.140.137.57  nfs3     vol1      pol1     6m 51s       14         0
10.140.137.57  nfs4     vol1      pol1     5s           16         0

3 entries were displayed.
```

vserver nfs credentials count

Count credentials cached by NFS

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

Description

The `vserver nfs credentials count` command displays the number of credentials stored in NFS credentials cache on a specific node. This command has no effect if the specified node has no active data.

Parameters

-node <nodename> - Node (privilege: advanced)

The name of the node on which the command is executed.

Examples

Lists the number of credentials stored by NFS on node node1

```
cluster1::*> vserver nfs credentials count -node node1

Number of credentials cached by NFS on node "node1": "2"
```

vserver nfs credentials flush

Flush credentials cached by NFS

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

Description

The `vserver nfs credentials flush` command deletes credentials from the NFS credentials cache on a specific node for a given Vserver or a given UNIX user. This command has no effect if the vserver that is specified has no active data interfaces on the node where the command is run.

Parameters

-node <nodename> - Node (privilege: advanced)

The name of the node on which the command is executed.

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

Use this parameter to clear the credential cache for the Vserver you specify.

{ [-unix-user-id <integer>] - UNIX User ID (privilege: advanced)

Use this parameter to clear the credential cache for the UNIX user id you specify.

[-client-ip <IP Address>] - Client IP Address (privilege: advanced)

Use this parameter to clear the credential cache for the client IP address you specify.

| [-unix-user-name <text>] - UNIX User Name (privilege: advanced)

Use this parameter to clear the credential cache for the UNIX user name you specify.

| [-unix-group-id <integer>] - UNIX Group ID (privilege: advanced)

Use this parameter to clear the credential cache for the UNIX group id you specify.

| [-unix-group-name <text>] - UNIX Group Name (privilege: advanced) }

Use this parameter to clear the credential cache for the UNIX group name you specify.

Examples

Clear the credential cache for user user1 on node node1 in Vserver vs1.

```
cluster1::*> vserver nfs credentials flush -node node1 -vserver vs1 -unix
-user-name user1

Number of matching credentials flushed: 1
```

vserver nfs credentials show

Show credentials cached by NFS

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

Description

The `vserver nfs credentials show` command displays the user account credentials stored on a specific node for a given UNIX user. This command has no effect if the vserver specified has no active data interfaces on the node where the command is run.

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> - Node (privilege: advanced)

The name of the node on which the command is executed.

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

Use this parameter to search for user credentials in the Vserver you specify.

{ -unix-user-id <integer> - UNIX User ID (privilege: advanced)

Use this parameter to search for user credentials for the UNIX user id you specify.

[-client-ip <IP Address>] - Client IP Address (privilege: advanced)

Use this parameter to search for user credentials for the client ip you specify.

| -unix-user-name <text> - UNIX User Name (privilege: advanced)

Use this parameter to search for user credentials for the UNIX user name you specify.

| -unix-group-id <integer> - UNIX Group ID (privilege: advanced)

Use this parameter to search for user credentials for the UNIX group id you specify.

| -unix-group-name <text> - UNIX Group Name (privilege: advanced) }

Use this parameter to search for user credentials for the UNIX group name you specify.

[-flags {ip-qualifier-configured|ip-qualifier-not-configured|unix-extended-creds-present|no-unix-extended-creds|unix-extended-creds-requested|unix-creds-transient-failure|cifs-creds-present|no-cifs-creds|cifs-creds-requested|cifs-cifs-transient-failure|place-holder|transient-failure|transient-error-on-last-refresh|id-name-mapping-present|no-id-name-mapping|id-name-mapping-requested|id-name-mapping-transient-failure|unix-cred-is-partial}] - Credential Entry Flags (privilege: advanced)

The credential entry flags.

[-last-refresh-time <[<integer>h][<integer>m][<integer>s]>] - Time since Last Refresh (privilege: advanced)

Time since last refreshed.

[-last-access-time <[<integer>h][<integer>m][<integer>s]>] - Time since Last Access (privilege: advanced)

Time since last access.

[-hit-count <integer>] - Number of Hits (privilege: advanced)

Number of times the cached credential is fetched successfully.

[-unix-cred-flags <integer>] - UNIX Credential Flags (privilege: advanced)

UNIX credentials flags.

[-unix-cred-domain-id <integer>] - UNIX Credential Domain ID (privilege: advanced)

UNIX credentials domain ID.

[-unix-cred-uid <integer>] - UNIX Credential UID (privilege: advanced)

User ID of the UNIX user.

[-unix-cred-primary-gid <integer>] - UNIX Credential Primay GID (privilege: advanced)

Primary GID of the UNIX user.

[-unix-cred-additional-gids <integer>,…] - UNIX Credential Additional GIDs (privilege: advanced)

Additional GIDs of the UNIX user.

[-win-cred-flags <integer>] - Windows Credential Flags (privilege: advanced)

Windows credentials flags.

[-win-cred-user-sid <text>] - Windows Credential User SID (privilege: advanced)

SID of the windows user.

[-win-cred-primary-group-sid <text>] - Windows Credential Primary Group SID (privilege: advanced)

SID of the windows user’s primary group.

[-win-cred-domain-sids <text>,…] - Windows Credential Domain SIDs (privilege: advanced)

Domain SIDs of the windows user.

Examples

Show the credentials cached by NFS Cred Store for the UNIX user node1 on node node1.

```
gnk1cluster1::*> vserver nfs credentials show -node gnk1cluster1-01
-vserver coke -unix-user-name root

Credentials
 -----------
                     Node: gnk1cluster1-01
                  Vserver: coke
                Client IP: -
                    Flags: ip-qualifier-not-configured, unix-extended-
creds-present, cifs-creds-present, id-name-mapping-present
  Time since Last Refresh: 10s
   Time since Last Access: 5s
                Hit Count: 24
Unix Credentials:
                    Flags: 0
                Domain ID: 0
                      UID: 0
              Primary GID: 1
          Additional GIDs: 1
Windows Credentials:
                    Flags: 8759
                 User SID: S-1-5-21-2552784647-1202982559-4146209732-500
        Primary Group SID: S-1-5-21-2552784647-1202982559-4146209732-513
              Domain SIDs: S-1-5-21-2552784647-1202982559-4146209732
                           S-1-1
                           S-1-5
                           S-1-5-32
ID-Name Information:
                     Type: user
                       ID: 0
                     Name: root
```

vserver nfs kerberos interface disable

Disable NFS Kerberos on a LIF

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

Description

The `vserver nfs kerberos interface disable` command disables NFS Kerberos on a logical interface.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the Vserver in which the logical interface exists.

`-lif <lif-name>` - Logical Interface
This parameter specifies the name of the logical interface on which you want to disable NFS Kerberos.

`[-admin-username <text>]` - Account Creation Username
This optional parameter specifies the administrator user name.

`[-admin-password <text>]` - Account Creation Password
This optional parameter specifies the administrator password.

Examples

The following example disables NFS Kerberos on a Vserver named vs0 and a logical interface named datalif1.

```
vs1::> vserver nfs kerberos interface disable -vserver vs0 -lif datalif1
```

vserver nfs kerberos interface enable

Enable NFS Kerberos on a LIF

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

Description

The `vserver nfs kerberos interface enable` command enables NFS Kerberos on a logical interface.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the Vserver in which the logical interface exists.

`-lif <lif-name>` - Logical Interface
This parameter specifies the name of the logical interface on which you want to enable NFS Kerberos.

`[-spn <text>]` - Service Principal Name
This optional parameter specifies the service principal name (SPN) for the logical interface you want to enable. 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 name in uppercase.

[-admin-username <text>] - Account Creation Username

This optional parameter specifies the administrator user name.

[-admin-password <text>] - Account Creation Password

This optional parameter specifies the administrator password.

[-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.

[-ou <text>] - Organizational Unit

This optional parameter specifies the organizational unit (OU) under which the Microsoft Active Directory server account will be created when you enable Kerberos using a realm for Microsoft KDC. If this parameter is not specified, the default OU is "CN=Computers".

[-machine-account <text>] - Machine Account Name

This optional parameter specifies the machine account to create in Active Directory

Examples

The following example enables NFS Kerberos 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 interface enable -vserver vs0 -lif datalif1
-spn nfs/sec.example.com@AUTH.SEC.EXAMPLE.COM -keytab-uri
 ftp://ftp.example.com/keytab
```

vserver nfs kerberos interface 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 interface 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 <text> - 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.

[-ou <text>] - Organizational Unit

This optional parameter specifies the organizational unit (OU) under which the Microsoft Active Directory server account will be created when you enable Kerberos using a realm for Microsoft KDC. If this parameter is not specified, the default OU is "CN=Computers".

[-machine-account <text>] - Machine Account Name

This optional parameter specifies the machine account to create in Active Directory

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 interface 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 interface 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 interface 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 permitted encryption types

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 <text>] - 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.

[-permitted-enc-types <NFS Kerberos Encryption Type>,…] - Permitted Encryption Types

If you specify this parameter, the command displays information only about the Kerberos configuration for NFS that matches the specified encryption types.

[-machine-account <text>] - Machine Account Name

If you specify this parameter, the command displays information only about the Kerberos configuration for NFS that matches the specified machine account.

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 interface show -vserver vs0 -lif datalif1
                   Vserver: vs1
         Logical Interface: datalif1
                IP Address: 192.0.2.130
          Kerberos Enabled: enabled
    Service Principal Name: nfs/sec.example.com@AUTH.SEC.EXAMPLE.COM
Permitted Encryption Types: des,des3,aes-128,aes-256
```

vserver nfs kerberos realm create

Create a Kerberos realm configuration

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

Description

The `vserver nfs kerberos realm create` command creates a Kerberos realm configuration.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver associated with 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 named SEC.EXAMPLE.COM for the Vserver named AUTH. 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 nfs kerberos realm create -vserver 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 nfs kerberos realm delete

Delete a Kerberos realm configuration

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

Description

The `vserver nfs kerberos realm delete` command deletes a Kerberos realm configuration from the system.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for the Kerberos realm configuration that you want to delete.

`-realm <text>` - Kerberos Realm

This parameter specifies the name of the Kerberos realm for the configuration.

Examples

The following example deletes the Kerberos realm SEC.EXAMPLE.COM from the Vserver named AUTH:

```
cluster1::> vserver nfs kerberos realm delete -vserver AUTH -realm
SEC.EXAMPLE.COM
```

vserver nfs kerberos realm modify

Modify a Kerberos realm configuration

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

Description

The `vserver nfs kerberos realm modify` command modifies one or more attributes of a Kerberos realm configuration.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for 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 SEC.EXAMPLE.COM for the Vserver 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::> vserver nfs kerberos realm modify -vserver AUTH -realm
SEC.EXAMPLE.COM -adserver-name AUTH.SEC.EXAMPLE.COM -adserver-ip
192.0.2.170 -kdc-ip 192.0.2.170 -kdc-vendor Microsoft
```

vserver nfs kerberos realm show

Display Kerberos realm configurations

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

Description

The `vserver nfs 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:

- Vserver
- Kerberos realm name
- Active Directory server name
- Kerberos Distribution Center (KDC) vendor
- KDC IP address
- The permitted encryption types

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 Kerberos realm configurations for the specified Vserver.

[-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.

[-permitted-enc-types <NFS Kerberos Encryption Type>,…] - Permitted Encryption Types

If you specify this parameter, the command displays information only about the Kerberos realm configuration that match the specified encryption types.

Examples

The following example displays information about all Kerberos realm configurations:

```
cluster1::> vserver nfs kerberos realm show
Kerberos                 Active Directory KDC        KDC
Vserver  Realm                    Server           Vendor     IP Address
-------- ------------------------ ---------------- ----------
-----------------
AUTH     SEC.EXAMPLE.COM          AUTH.SEC.EXAMPLE.COM
                                                   Microsoft  192.0.2.170
```

vserver nfs pnfs devices create

Create a new pNFS device and its mapping

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

Description

```
The `vserver nfs pnfs devices create` command creates a pNFS device for a
given instance of a volume. The actual creation of pNFS devices is
automatically done by the pNFS implementation in Data ONTAP kernel. The
usage of this command might interfere with the functionality of the pNFS
server. Thus, it is advised that this command not be used without
supervision by technical support.
```

Parameters

`[-global-device-table-id <integer>]` - Global Device Mapping Table ID (privilege: advanced)

This optional parameter specifies the unique identifier that the pNFS devices subsystem assigns to the device that corresponds to the MSID described below. The pNFS devices implementations keeps track of the global unique identifier that needs to be assigned to this device. It is expected that users need not specifically input the device identifier while creation.

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

This parameter specifies the Vserver to which the volumes belong.

`-msid <integer>` - Volume MSID (privilege: advanced)

This parameter uniquely identifies the volume for which you are creating a pNFS device.

`-striping-epoch <integer>` - Striping Epoch (privilege: advanced)

This optional parameter specifies the striping epoch identifier for a volume for which you are creating a pNFS device. For flexible volumes, the value is always 1.

`-device-access <integer>` - Device Access Flags (privilege: advanced)

This optional parameter specifies the type of access that is given to the pNFS device that you are creating. If the value is 1, it means write access. If the value if 0, it means read access. By default, the device is created with write access.

`-version <integer>` - Device Version (privilege: advanced)

This optional parameter specifies the version associated with the pNFS device identifier. By default, the version is set to 1.

`[-generation-count <integer>]` - Device Generation (privilege: advanced)

This optional parameter specifies the generation count associated with the pNFS device identifier. If a device already exists, the existing device is invalidated and the generation number for the device is bumped. If a device does not already exist, a new device is created with generation number 1.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Device Creation Time (privilege: advanced)

This optional parameter specifies the time at which the device is created. If the parameter is not specified, the time at which the device is created is stored along with the device.

[-mapping-status {available|notavailable}] - Device Mapping Status (privilege: advanced)

This optional parameter specifies if the mapping exists for a device. If the value is set to "available", the mappings will be created in the device mappings table. If the value is set to "notavailable", the mappings will not be created in the device mappings table.

Examples

vserver nfs pnfs devices delete

Delete a pNFS device

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

Description

The `vserver nfs pnfs devices delete` command deletes a unique pNFS device. The pNFS device to be deleted is identified by the unique device mapping identifier (mid) parameter passed to this operation. When this operation is successful, the device mappings corresponding to the device and the information corresponding to the device itself are removed. You can obtain the global mapping identifier from the list of devices using the command vserver nfs pnfs devices show .

Parameters

-global-device-table-id <integer> - Global Device Mapping Table ID (privilege: advanced)

This parameter specifies the pNFS global device mapping identifier that uniquely identifies a pNFS device

Examples

The following example deletes the device information of a device with global mapping identifier value 2.

```
cluster1::> vserver nfs pnfs delete -mid 2
```

Related Links

- vserver nfs pnfs devices show

vserver nfs pnfs devices show

Display pNFS device information

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

Description

The `vserver nfs pnfs devices show` command displays a pNFS device for a given instance of a volume. 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 pNFS devices:

- Vserver name
- The global device mapping identifier of the device
- The master data set ID (MSID) of the volume that leads to this device
- The mapping status of the device
- The generation number of the device

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about devices that are exported as write-only devices, enter the command with the `-access-flags 1` 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.

[-global-device-table-id <integer>] - Global Device Mapping Table ID (privilege: advanced)

If you specify this parameter, the command displays information only about the unique identifier that the pNFS devices subsystem assigns to the device that is being output.

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

If you specify this parameter, the command displays information only about the Vserver that owns the volume represented by MSID.

[-msid <integer>] - Volume MSID (privilege: advanced)

If you specify this parameter, the command displays information only about the volume or volumes that match the specified MSID.

[-striping-epoch <integer>] - Striping Epoch (privilege: advanced)

If you specify this parameter, the command displays information only about the striping epoch identifier for a volume that serves as the basis for the pNFS device.

[-device-access <integer>] - Device Access Flags (privilege: advanced)

If you specify this parameter, the command displays information only about access flags which specify the type of access that is given to the pNFS device. If the value is 1, it means write access. If the value is 0, it means read access.

[-version <integer>] - Device Version (privilege: advanced)

If you specify this parameter, the command displays information only about pNFS devices that match the specified version number.

[-generation-count <integer>] - Device Generation (privilege: advanced)

If you specify this parameter, the command displays information only about generation count associated with the pNFS device identifier.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Device Creation Time (privilege: advanced)

If you specify this parameter, the command displays information only about pNFS devices that were created at the specified time.

[-mapping-status {available|notavailable}] - Device Mapping Status (privilege: advanced)

If you specify this parameter, the command displays information only about if the mapping exists for a device. If the value is set to "available", the mappings can be seen in the device mappings table. If the value is set to "notavailable", the mappings will not be seen in the device mappings table.

Examples

The following example displays the information of a device with global mapping identifier 6. The device corresponds to a volume with MSID 2147484673 on Vserver vs1. The device mappings corresponding to this device follow in the mappings table.

```
cluster1::*> vserver nfs pnfs devices show
Vserver Name     Mapping ID      Msid            Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
vs1              1               2147484673      available       6

cluster1::*> vserver nfs pnfs devices mappings show
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
vs1             1               1025            10.53.4.14
```

vserver nfs pnfs devices cache show

Display the device cache

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

Description

```
The `vserver nfs pnfs devices cache show` command displays the device
cache.
```

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.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays information only about the pNFS devices cache present on the node.

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

If you specify this parameter, the command displays information only about the Vserver that has the pNFS devices cache.

Examples

vserver nfs pnfs devices mappings show

Display the list of pNFS device mappings

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

Description

```
The xref:{relative_path}vserver-nfs-pnfs-devices-show.html[vserver nfs
pnfs devices show] command displays a pNFS device for a given instance of
a volume. The command output depends on the parameter or parameters
specified with the command. If you do not specify parameters, the command
displays the following information about all pNFS devices:
```

- Vserver name
- The global device mapping identifier of the device
- The Data Set ID (DSID) of the constituent volume
- The LIF IP address that serves the constituent on the same controller.

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about devices that are exported as write-only devices, enter the command with the `-access-flags 1` 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.

[-global-device-table-id <integer>] - Global Device Mapping Table ID (privilege: advanced)

This specifies the unique identifier that the pNFS devices subsystem assigns to the device whose mappings are being output.

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

If your specify this parameter, the command displays information only about the Vserver that the mapping identifier and DSID belong to.

[-dsid <integer>] - Constituent Volume DSID (privilege: advanced)

If you specify this parameter, the command displays information only about the volume or volumes that match the specified DSID.

[-lifip <IP Address>] - LIF IP Address (privilege: advanced)

If you specify this parameter, the command displays information only about the pNFS devices that match the specified LIF IP address.

Examples

The following example displays the device information of a device with global mapping identifier 6. The device corresponds to a volume with MSID 2147484673 on Vserver vs1. The device has one constituent with DSID 1025 and is served by the LIF with the IP address 10.53.4.14.

```
cluster1::*> vserver nfs pnfs devices* show
Vserver Name     Mapping ID      Msid            Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
vs1              1               2147484673      available       6

cluster1::*> vserver nfs pnfs devices mappings show
Vserver Name    Mapping ID      Dsid            Lif IP
--------------  --------------- --------------- --------------------
vs1             1               1025            10.53.4.14
```

Related Links

- vserver nfs pnfs devices show

vserver nvme commands

vserver nvme create

Create NVMe service configuration

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

Description

The `vserver nvme create` command creates an NVMe service for a Vserver.

When you create the NVMe service on a Vserver, the Vserver must have only *`nvme`* in the allowed-protocols list.

When you create the NVMe service on a Vserver, the administrative status of the service is *`up`* by default.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver for the NVMe service.

`[-status-admin {down|up}]` - Administrative Status
Specifies the configured administrative status of a service.

Examples

```
cluster1::*> vserver nvme create -vserver vs_1
```

Creates an NVMe service on Vserver *`vs_1`* .

vserver nvme delete

Delete NVMe service configuration

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

Description

The `vserver nvme delete` command deletes an NVMe service of a Vserver. Before you can delete an NVMe service, the administrative status must be *`down`* . Use the vserver nvme modify command to change the administrative status.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver for the NVMe service.

Examples

```
cluster1::*> vserver nvme delete -vserver vs_1
```

Deletes the NVMe service on Vserver *`vs_1`* .

Related Links

- vserver nvme modify

vserver nvme modify

Modify NVMe service configuration

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

Description

The `vserver nvme modify` command modifies an NVMe service configuration on a Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver for the NVMe service.

`[-status-admin {down|up}]` - Administrative Status

Specifies the configured administrative status of a service. If you set this parameter to *`down`* , the Vserver will not serve NVMe traffic.

Examples

```
cluster1::*> vserver nvme modify -vserver vs_1 -status-admin down
```

Sets the adminitrative status of the NVMe service on Vserver *`vs_1`* to *`down`* .

vserver nvme show-interface

Display the NVMe over Fabrics LIF configuration

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

Description

The `vserver nvme show-interface` command displays the currently available interfaces to the NVMe protocol.

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 NVMe interfaces that match the Vserver that you specify.

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

Use this parameter to display the NVMe interfaces that match the LIF that you specify.

[-vserver-uuid <UUID>] - Vserver UUID

Use this parameter to display the NVMe interfaces that match the Vserver UUID that you specify.

[-home-node <nodename>] - Home Node

Use this parameter to display the NVMe interfaces that match the home node that you specify.

[-home-port {<netport>|<ifgrp>}] - Home Port

Use this parameter to display the NVMe interfaces that match the home port that you specify.

[-status-admin {up|down}] - Status Admin

Use this parameter to display the NVMe interfaces that match the administrative status that you specify.

[-physical-protocol {fibre-channel|ethernet}] - Physical Protocol

Use this parameter to display the NVMe interfaces that match the physical protocol that you specify.

[-transport-protocol {fc-nvme|nvme-roce}] - Transport Protocol

Use this parameter to display the NVMe interfaces that match the transport protocol that you specify.

[-transport-address <text>] - Transport Address

Use this parameter to display the NVMe interfaces that match the transport address that you specify.

[-comment <text>] - Comment

Use this parameter to display the NVMe interfaces that match the textual comment that you specify.

[-fc-wwnn <FC WWN>] - FC WWNN

Use this parameter to display the NVMe interfaces that match the FC WWNN that you specify.

[-fc-wwpn <FC WWN>] - FC WWPN

Use this parameter to display the NVMe interfaces that match the FC WWPN that you specify.

[-lif-id <integer>] - LIF ID

Use this parameter to display the NVMe interfaces that match the LIF ID that you specify.

[-lif-uuid <UUID>] - LIF UUID

Use this parameter to display the NVMe interfaces that match the LIF UUID that you specify.

Examples

```
cluster1::*> vserver nvme show-interface
Vserver Logical Interface    Home Node:Port     Transport Protocols
------- -------------------- ------------------
----------------------------
vs_1
        nvme1                node1:1a           fc-nvme
          Transport Address: nn-0x2000005056b45113:pn-0x2001005056b45113
```

vserver nvme show

Show NVMe service configuration

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

Description

The `vserver nvme show` command displays the current status of the NVMe 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 NVMe services that match the Vserver that you specify.

[-status-admin {down|up}] - Administrative Status

Use this parameter to display the NVMe services that match the administrative status that you specify.

Examples

```
cluster1::*> vserver nvme show
Vserver    Status Admin
---------- ------------
vs1        up
vs2        up
2 entries were displayed.
```

vserver nvme feature show

Display NVMe target features

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

Description

Displays the list of currently enabled NVMe over Fabrics features and limits.

Examples

```
cluster1::*> vserver nvme feature show
      Enabled Features: nvmf, fc-nvme, multi-path, multi-node
Maximum Namespace Size: 15.97TB
          Maximum NSID: 00000200h
      Maximum ANAGRPID: 00000200h
```

vserver nvme namespace create

Create an NVMe namespace

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

Description

The `vserver nvme namespace create` command creates a new NVMe namespace of a specific size. You must create NVMe namespaces at the root of a volume or qtree.

When you create an NVMe namespace, it is non-space reserved.

This command is not supported for FlexGroups or Vservers with Infinite Volumes.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver.

`-path <path>` - Namespace Path

Specifies the path of the NVMe namespace. Examples of correct NVMe namespace paths are */vol/vol1/ns1* and */vol/vol1/qtree1/ns1* .

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

Specifies the size of the NVMe namespace in bytes. You can specify a multiplier suffix:

- KB (1024 bytes)
- MB (KB*KB bytes)
- GB (KB*MB bytes)
- TB (MB*MB bytes)

`-ostype {vmware|windows|linux}` - OS Type

Specifies the operating system type of the NVMe namespace. The OS types are:

- linux - the NVMe namespace stores Linux file system data.
- vmware - the NVMe namespace stores VMware file system data.
- windows - the NVMe namespace stores Windows file system data.

[-comment <text>] - Comment

Contains a textual description of the NVMe namespace.

[-block-size {512|4KB}] - Block Size

Specifies the block size of the NVMe namespace in bytes. Valid block sizes are

- *512* (in Data ONTAP 9.6 and later)
- *4096*

Examples

```
cluster1::*> vserver nvme namespace create -vserver vs_1 -path
/vol/nsvol/namespace1 -size 100g -ostype linux
```

Creates an NVMe namespace at path */vol/ns/vol/namespace1* on Vserver *vs_1* .

vserver nvme namespace delete

Delete an NVMe namespace

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

Description

The `vserver nvme namespace delete` command deletes an NVMe namespace from a specified Vserver and volume.

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver.

-path <path> - Namespace Path

Specifies the path of the NVMe namespace. Examples of correct NVMe namespace paths are */vol/vol1/ns1* and */vol/vol1/qtree1/ns1* .

[-skip-mapped-check <true>] - Skip Mapped Check

This option is required to delete an NVMe namespace that is attached to a subsystem.

Examples

```
cluster1::*> vserver nvme namespace delete -vserver vs1 -path
/vol/nsvol/ns1
```

Deletes the NVMe namespace at path */vol/nsvol/ns1* on Vserver *vs1* .

vserver nvme namespace modify

Modify an NVMe namespace

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

Description

The `vserver nvme namespace modify` command modifies NVMe namespace attributes.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver.

`-path <path>` - Namespace Path
Specifies the path of the NVMe namespace. Examples of correct NVMe namespace paths are */vol/vol1/ns1* and */vol/vol1/qtree1/ns1* .

`[-comment <text>]` - Comment
Contains a textual description of the NVMe namespace.

Examples

```
cluster1::*> vserver nvme namespace modify -path /vol/nsvol/ns1 -vserver
vs_1 -comment "Comment text."
```

Modifies the value of the comment field for the NVMe namespace at path */vol/nsvol/ns1* on Vserver *vs_1* .

vserver nvme namespace show

Display NVMe namespaces

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

Description

The `vserver nvme namespace show` command displays information for NVMe namespaces.

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 NVMe namespaces that match the Vserver that you specify.

[-path <path>] - Namespace Path

Use this parameter to display the NVMe namespace that matches the path that you specify.

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

Use this parameter to display the NVMe namespaces that match the size that you specify.

[-size-used {<integer>[KB|MB|GB|TB|PB]}] - Size Used

Use this parameter to display the NVMe namespaces that match this parameter value.

[-ostype {vmware|windows|linux}] - OS Type

Use this parameter to display the NVMe namespaces that match this parameter value.

[-comment <text>] - Comment

Use this parameter to display the NVMe namespaces that match this parameter value.

[-block-size {512|4KB}] - Block Size

Use this parameter to display the NVMe namespaces that match this parameter value.

[-state {online|offline|nvfail|space-error}] - State

Use this parameter to display the NVMe namespaces that match this parameter value.

[-is-read-only {true|false}] - Is Read Only

Use this parameter to display the NVMe namespaces that match this parameter value.

[-creation-timestamp <MM/DD/YYYY HH:MM:SS>] - Creation Time

Use this parameter to display the NVMe namespaces that match this parameter value.

[-uuid <UUID>] - Namespace UUID

Use this parameter to display the NVMe namespaces that match this parameter value.

[-restore-inaccessible {true|false}] - Restore Inaccessible

Use this parameter to display the NVMe namespaces that match this parameter value.

[-node <nodename>] - Node Hosting the Namespace

Use this parameter to display the NVMe namespaces that match this parameter value.

[-volume <volume name>] - Volume Name

Use this parameter to display the NVMe namespaces that match this parameter value.

[-qtree <qtree name>] - Qtree Name

Use this parameter to display the NVMe namespaces that match this parameter value.

[-subsystem <text>] - Mapped Subsystem

Use this parameter to display the NVMe namespaces that are attached to a Subsystem that matches this parameter value.

[-nsid <Hex 32bit Integer>] - Namespace ID

Use this parameter to display the NVMe namespaces that match this parameter value.

[-anagrpid <Hex 32bit Integer>] - ANA Group ID (privilege: advanced)

Use this parameter to display the NVMe namespaces that match Asymmetric Namespace Access (ANA) group identifier that you specify.

[-vserver-id <integer>] - Vserver ID

Use this parameter to display the NVMe namespaces that match this parameter value.

[-container-state {online|aggregate-offline|volume-offline|error}] - Namespace Container State (privilege: advanced)

Selects the namespaces that match this parameter value. The container states are:

- *online* - The namespace's aggregate and volume are online.
- *aggregate-offline* - The namespace's aggregate is offline.
- *volume-offline* - The namespace's volume is offline.
- *error* - An error occurred accessing the namespace's volume.

[-include-offline-containers <true>] - Include Namespaces on Offline Volumes and Aggregates (privilege: advanced)

If true, include available information for namespaces in offline aggregates and offline volumes in the output. By default, namespaces in offline aggregates and offline volumes are excluded from the output.

[-application <text>] - Application

Selects the namespace that are part of an application that matches the parameter value.

Examples

```
cluster::*> vserver nvme namespace show -vserver vs1
Vserver   Path                            State     Size Subsystem
NSID
--------- ------------------------------- ------- ------ ----------
---------
vs1       /vol/test_1_vol/ns1             online    10GB subsys1
00000001h
vs1       /vol/test_1_vol/ns2             online   500MB subsys1
00000002h
vs1       /vol/test_1_vol/ns3             online     1TB -
-
3 entries were displayed.
```

vserver nvme subsystem create

Create an NVMe target subsystem

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

Description

The `vserver nvme subsystem create` command creates a new NVMe target subsystem.

When you create an NVMe subsystem on a Vserver, the Vserver must meet the following pre-conditions:

- The Vserver must have an NVMe service created.
- The Vserver must not already have an NVMe subsystem by the same name.

> The NVMe subsystem identifiers are assigned by the system. The NQN is derived from the Vserver UUID and subsystem name and may not be specified or modified by the user.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver.

`-subsystem <text>` - Subsystem

Specifies the NVMe target subsystem.

`-ostype {windows|linux|vmware}` - OS Type

Specifies the operating system type of the NVMe subsystem. The OS types are:

- linux - the initiators belong to a Linux host.
- vmware - the initiators belong to a VMware ESX host.
- windows - the initiators belong to a Windows host.

[-comment <text>] - Comment

Contains a textual description of the NVMe subsystem.

[-delete-on-unmap {true|false}] - Delete on Unmap (privilege: advanced)

Specifies whether the subsystem should be deleted automatically when it is no longer mapped to a namespace.

[-vendor-uuids <UUID>,…] - Vendor UUIDs (privilege: advanced)

Specifies vendor-specific identifiers (UUIDs) optionally assigned to an NVMe subsystem when the subsystem is created. The identifiers are used to enable vendor-specific NVMe protocol features. The identifiers are provided by a host application vendor and shared with NetApp prior to a joint product release. Creating an NVMe subsystem with an unknown or non-specific identifier will have no effect on the NVMe subsystem. Refer to the ONTAP SAN Administration Guide for a list of the supported vendor-specific identifiers. After a subsystem is created, the vendor-specific identifiers cannot be changed or removed.

Examples

```
cluster1::*> vserver nvme subsystem create -vserver vs_1 -subsystem sub_1
-ostype linux
```

Creates a subsystem named *sub_1* on Vserver *vs_1* .

vserver nvme subsystem delete

Delete the subsystem

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

Description

The `vserver nvme subsystem delete` command deletes an NVMe subsystem from a specified Vserver.

Parameters

-vserver <Vserver Name> - Vserver Name

Specifies the Vserver.

-subsystem <text> - Subsystem

Specifies the NVMe target subsystem.

[-skip-mapped-check <true>] - Skip Mapped Namespace Check

Required to delete an NVMe subsystem with attached NVMe namespaces.

[-skip-host-check <true>] - Skip Host Check

Required to delete an NVMe subsystem with associated hosts.

Examples

```
cluster1::*> vserver nvme subsystem delete -vserver vs_1 -subsystem sub_1
```

Deletes the NVMe subsystem *sub_1* on Vserver *vs_1* .

vserver nvme subsystem modify

Modify an NVMe target subsystem

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

Description

The `vserver nvme subsystem modify` command modifies an existing NVMe target subsystem.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver.

`-subsystem <text>` - Subsystem
Specifies the NVMe target subsystem.

`[-comment <text>]` - Comment
Contains a textual description of the NVMe subsystem.

`[-delete-on-unmap {true|false}]` - Delete on Unmap (privilege: advanced)
Specifies whether the subsystem should be deleted automatically when it is no longer mapped to a namespace.

Examples

```
cluster1::*> vserver nvme subsystem modify -vserver vs_1 -subsystem sub_1
-comment "Example Comment"
```

Modifies the comment on the subsystem named *sub_1* on Vserver *vs_1* .

vserver nvme subsystem show

Display NVMe target subsystems

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

Description

The `vserver nvme subsystem show` command displays information for NVMe subsystems.

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 NVMe subsystems that match the Vserver that you specify.

[-subsystem <text>] - Subsystem

Use this parameter to display the NVMe subsystem that matches the name that you specify.

[-ostype {windows|linux|vmware}] - OS Type

Use this parameter to display the NVMe subsystems that match this parameter value.

[-comment <text>] - Comment

Use this parameter to display the NVMe subsystems that match this parameter value.

[-target-nqn <text>] - Target NQN

Use this parameter to display the NVMe subsystems that match this parameter value.

[-serial-number <text>] - Serial Number

Use this parameter to display the NVMe subsystems that match this parameter value.

[-default-io-queue-count <integer>] - Default Number of Host I/O Queue Pairs

Specifies the default maximum IO queue count inherited by hosts added to this subsystem.

[-default-io-queue-depth <integer>] - Default Host I/O Queue Depth

Specifies the default maximum IO queue depth inherited by hosts added to this subsystem.

[-uuid <UUID>] - UUID

Use this parameter to display the NVMe subsystems that have UUIDs matching the parameter value.

[-delete-on-unmap {true|false}] - Delete on Unmap (privilege: advanced)

Specifies whether the subsystem should be deleted automatically when it is no longer mapped to a namespace.

[-vendor-uuids <UUID>,…] - Vendor UUIDs (privilege: advanced)

Use this parameter to display the NVMe subsystems that have vendor-specific UUIDs that match the parameter value.

Examples

```
cluster1::*> vserver nvme subsystem show -vserver vs_1
Vserver Subsystem    Target NQN
------- ------------
----------------------------------------------------
vs_1
        ss1          nqn.1992-
08.netapp.com:sn.ccb5a7d5d9d311e7924e005056b45113:subsystem.ss1
        ss2          nqn.1992-
08.netapp.com:sn.ccb5a7d5d9d311e7924e005056b45113:subsystem.ss2
2 entries were displayed.
```

vserver nvme subsystem controller show

Display active NVMe controllers

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

Description

The `vserver nvme subsystem controller show` command displays information for established NVMe controllers. An NVMe controller is established upon each host connection to a subsystem.

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 NVMe controllers that match the Vserver that you specify.

[-subsystem <text>] - Subsystem

Use this parameter to display the NVMe controllers that match the subsystem that you specify.

[-controller-id <Hex 16bit Integer>] - Controller ID

Use this parameter to display the NVMe controllers that match the controller ID that you specify. The controller ID is the identifier assigned by the NVMe subsystem upon host login and controller creation.

[-lif <text>] - Logical Interface

Use this parameter to display the NVMe controllers that match the LIF that you specify.

[-node <nodename>] - Node

Use this parameter to display the NVMe controllers that match the cluster node that you specify.

[-host-nqn <text>] - Host NQN

Use this parameter to display the NVMe controllers that match the host NQN that you specify. The host NQN is the NVMe identifier assigned to a specific host.

[-transport-protocol {fc-nvme|nvme-roce}] - Transport Protocol

Use this parameter to display the NVMe controllers that match the transport protocol that you specify.

[-initiator-transport-address <text>] - Initiator Transport Address

Use this parameter to display the NVMe controllers that match the initiator transport address that you specify. The initiator transport address format depends on the transport protocol in use.

[-host-id <Hex String>] - Host Identifier

Use this parameter to display the NVMe controllers that match the host identifier that you specify. The host identifier is a 128-bit identifier assigned to a specific host.

[-io-queue-count <integer>] - Number of I/O Queues

Use this parameter to display the NVMe controllers that match the I/O queue count that you specify.

[-io-queue-depth <integer>,…] - I/O Queue Depths

Use this parameter to display the NVMe controllers that match the I/O queue depth that you specify.

[-admin-queue-depth <integer>] - Admin Queue Depth

Use this parameter to display the NVMe controllers that match the administrative queue depth that you specify.

[-subsystem-uuid <UUID>] - Subsystem UUID

Use this parameter to display the NVMe controllers that match the Subsystem UUID that you specify.

Examples

```
cluster1::*> vserver nvme subsystem controller show -vserver vs_1
-subsystem ss1
Vserver Subsystem    ID LIF    Host NQN
------- --------- ----- ------
---------------------------------------------
vs_1    ss1
                  0003h lif1   nqn.2001-08.example.com:nvme:host1
                  0004h lif1   nqn.2001-08.example.com:nvme:host2
                  0009h lif2   nqn.2001-08.example.com:nvme:host1
                  000Ah lif2   nqn.2001-08.example.com:nvme:host2
4 entries were displayed.
```

vserver nvme subsystem host add

Add a host to a subsystem

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

Description

The `vserver nvme subsystem host add` command adds an FC-NVMe host to an NVMe subsystem on a Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver.

`-subsystem <text>` - Subsystem
Specifies the NVMe target subsystem.

`-host-nqn <text>` - Host NQN
Specifies the NVMe subsystem host NQN.

Examples

```
cluster::*> vserver nvme subsystem host add -vserver vs_1 -subsystem sub_1
-host-nqn nqn.2001-01.com.example:nvme-host1
```

Adds a host with the specified NQN to the NVMe subsystem *`sub_1`* on Vserver *`vs_1`* .

vserver nvme subsystem host remove

Remove a host from a subsystem

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

Description

The `vserver nvme subsystem host remove` command removes an FC-NVMe host from an NVMe subsystem on a Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver Name
Specifies the Vserver.

`-subsystem <text>` - Subsystem
Specifies the NVMe target subsystem.

`-host-nqn <text>` - Host NQN
Specifies the NVMe subsystem host NQN.

Examples

```
cluster::*> vserver nvme subsystem host remove -vserver vs_1 -subsystem
sub_1 -host-nqn nqn.2001-01.com.example:host1
```

Removes the host with the specified NQN from NVMe subsystem *sub_1* on Vserver *vs_1* .

vserver nvme subsystem host show

Display NVMe hosts configured to the subsystem

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

Description

The `vserver nvme subsystem host show` command displays information for the NVMe subsystem hosts.

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 NVMe subsystem hosts that match the Vserver that you specify.

[-subsystem <text>] - Subsystem

Use this parameter to display the NVMe subsystem hosts that match the subsystem that you specify.

[-host-nqn <text>] - Host NQN

Use this parameter to display the NVMe subsystem host that matches the subsystem host NQN that you specify.

[-io-queue-count <integer>] - Number of I/O Queue Pairs

Use this parameter to display the NVMe subsystem hosts that match the maximum IO queue count that you specify.

[-io-queue-depth <integer>] - I/O Queue Depth

Use this parameter to display the NVMe subsystem hosts that match the maxium IO queue depth that you specify.

Examples

```
cluster::*> vserver nvme subsystem host show -vserver vs_1 -subsystem
sub_1
Vserver Subsystem Host NQN
------- --------- ----------------------------------
vs_1    sub_1     nqn.2001-08.com.example:nvme:host1
                  nqn.2001-08.com.example:nvme:host2
                  nqn.2001-08.com.example:nvme:host3
3 entries were displayed.
```

vserver nvme subsystem map add

Add a namespace map

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

Description

The `vserver nvme subsystem map add` command creates an association on an NVMe namespace to an NVMe subsystem.

When you add an NVMe subsystem map, the following pre-conditions must hold:

- The NVMe namespace must not be already mapped to a different subsystem.
- There must be an FC-NVMe LIF on the NVMe namespace owning node.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver.

`-subsystem <text>` - Subsystem

Specifies the NVMe target subsystem.

`-path <path>` - Namespace Path

Specifies the path of the NVMe namespace. Examples of correct NVMe namespace paths are */vol/vol1/ns1* and */vol/vol1/qtree1/ns1* .

Examples

```
cluster::*> vserver nvme subsystem map add -vserver vs_1 -subsystem sub_1
-path /vol/nsvol/namespace1
```

Adds an association on the NVMe namespace at the specified path to NVMe subsystem *sub_1* on Vserver *vs_1* .

vserver nvme subsystem map remove

Remove a namespace map

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

Description

The `vserver nvme subsystem map remove` command deletes an association on an NVMe namespace to an NVMe subsystem.

Parameters

`-vserver <Vserver Name>` - Vserver Name

Specifies the Vserver.

`-subsystem <text>` - Subsystem

Specifies the NVMe target subsystem.

`-path <path>` - Namespace Path

Specifies the path of the NVMe namespace. Examples of correct NVMe namespace paths are */vol/vol1/ns1* and */vol/vol1/qtree1/ns1* .

Examples

```
cluster::*> vserver nvme subsystem map remove -vserver vs_1 -subsystem
sub_1 -path /vol/nsvol/namespace1
```

Removes the association on the NVMe namespace at the specified path to NVMe subsystem *sub_1* on Vserver *vs_1* .

vserver nvme subsystem map show

Display namespace maps within the subsystem

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

Description

The `vserver nvme subsystem map show` command displays information about NVMe subsystem maps.

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 NVMe subsystem maps that match the Vserver that you specify.

[-subsystem <text>] - Subsystem

Use this parameter to display the NVMe subsystem maps that match the subsystem that you specify.

[-nsid <Hex 32bit Integer>] - NSID

Use this parameter to display the NVMe subsystem maps that match the NVMe namespace NSID that you specify.

[-path <path>] - Namespace Path

Use this parameter to display the NVMe subsystem maps that match the NVMe namespace path that you specify.

[-anagrpid <Hex 32bit Integer>] - ANA Group ID (privilege: advanced)

Use this parameter to display the NVMe namespaces that match the Asymmetric Namespace Access (ANA) group identifier that you specify.

[-namespace-uuid <UUID>] - Namespace UUID

Use this parameter to display the NVMe ubsystem maps that match the NVMe namespace UUID that you specify.

Examples

```
cluster-1::*> vserver nvme subsystem map show -vserver vs_1
Vserver       Subsystem      NSID Namespace Path
------------- --------- ---------
----------------------------------------
vs_1          sub_1
                         00000001h /vol/nsvol1/ns1
                         00000002h /vol/nsvol1/ns2
2 entries were displayed.
```

vserver object-store-server commands

vserver object-store-server create

Create an object store server

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

Description

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

Parameters

-vserver <vserver name> - Vserver

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

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

This parameter specifies the name of the object store server.

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

This optional parameter specifies if server should accept HTTP connections.

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

This optional parameter specifies if server should accept HTTPS connections.

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

Common name of the certificate used for HTTPS connections.

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

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

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

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

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

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

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

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

Examples

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

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

vserver object-store-server delete

Delete an object store server

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

Description

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

Parameters

-vserver <vserver name> - Vserver

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

Examples

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

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

vserver object-store-server modify

Modify an object store server

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

Description

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

Parameters

-vserver <vserver name> - Vserver

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

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

This parameter specifies the name of the object store server.

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

This optional parameter specifies if server should accept HTTP connections.

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

This optional parameter specifies if server should accept HTTPS connections.

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

Common name of the certificate used for HTTPS connections.

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

This parameter specifies the listener port for the object store server.

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

This parameter specifies the secure listener port for the object store server.

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

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

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

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

Examples

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

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

vserver object-store-server show

Display object store servers

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <vserver name>] - Vserver

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example displays information of all object store servers:

```
cluster1::> vserver object-store-server show
Vserver: vs3
Object Store Server Name: test.s3.local
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                    HTTP Enabled: false
                                   HTTPS Enabled: true
              Certificate for HTTPS Connections: server_cert
                                         Comment: Server comment
```

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

```
cluster1::> vserver object-store-server show -vserver vs1
Vserver: vs1
Object Store Server Name: test.s3.local
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                    HTTP Enabled: false
                                   HTTPS Enabled: true
              Certificate for HTTPS Connections: server_cert
                                         Comment: Server comment
```

vserver object-store-server bucket create

Create an object store server bucket

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

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

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

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

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

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

Use this parameter to specify the list of aggregates for the flexgroup constituents on which the bucket needs to be created.

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

Use this parameter to specify the number of flexgroup constituents to be created.

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

Use this parameter to specify if the bucket is going to be used for capacity tier.

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

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

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

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

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

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

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

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

Examples

vserver object-store-server bucket delete

Delete an object store bucket

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

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

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

Examples

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

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

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

Evict remote read-write cached objects

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

Description

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

Parameters

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

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

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

This specifies the name of the object store server bucket.

Examples

The following example starts the command:

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

vserver object-store-server bucket modify

Modify an object store server bucket

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

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

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

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

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

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

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

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

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

Examples

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

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

vserver object-store-server bucket show

Display object store server buckets

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
cluster1::> vserver object-store-server bucket show
Vserver     Bucket          Volume            Size       Encryption
----------- --------------- ----------------- ---------- ----------
vs1         testbucket1     fg_oss_1563344831 10GB       false
 Comment: test1
vs2         testbucket2     fg_oss_1563518684 1GB        false
 Comment: test2
2 entries were displayed.
```

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

```
cluster1::> vserver object-store-server bucket show -vserver vs1
Vserver     Bucket          Volume            Size       Encryption
----------- --------------- ----------------- ---------- ----------
vs1         testbucket      fg_oss_1563344831 10GB       false
 Comment: test1
```

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

```
cluster1::> vserver object-store-server bucket show -vserver vs1 -instance
Vserver: vs1
Bucket            :testbucket
  Uuid              :ef6c93db-a85b-11e9-b6dd-0050568e56f5
  Volume            :fg_oss_1563344831
  Size              :10GB
  Logical Used Size :7GB
  Object Count      :13
  Encryption        :false
  Comment           :test1
  Qos Group Policy  :qos
```

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

Create a bucket policy statement condition

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

Description

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

Parameters

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

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

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

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

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

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

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

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

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

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

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

Use this parameter to specify a list of object store server users for which the access will be allowed or denied based on the operator specified.

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

Use this parameter to specify a list of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

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

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

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

Use this parameter to specify a list of delimiters that are compared with the input delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.

Examples

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

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

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

Delete a bucket policy statement condition

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

Description

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

Parameters

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

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

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

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

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

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

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

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

Examples

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

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

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

Modify a bucket policy statement condition

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

Description

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

Parameters

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

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

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

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

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

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

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

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

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

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

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

Use this parameter to specify a list of object store server users for which the access will be allowed or denied based on the operator specified.

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

Use this parameter to specify a list of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

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

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

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

Use this parameter to specify a list of delimiters that are compared with the input delimiter value specified at

the time of execution of an S3-based command, using the condition operator specified.

Examples

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

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

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

Show the bucket policy condition

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Index Operator     Source-IPs    Usernames    Prefixes     Max-Keys
Delimiters
----- ------------ ------------- ------------ ------------ --------
-----------
    1 ip-address   1.1.1.0/24    -            -                  - -
    1 string-like  -             user1        pref               - delim1
2 entries were displayed.
```

vserver object-store-server bucket policy statement create

Create a bucket policy statement

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

Description

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

Parameters

-vserver <Vserver Name> - Vserver Name

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

-bucket <TextNoCase> - Object Store Server Bucket Name

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

[-index <integer>] - Statement Index

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

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

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

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

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads and ListMultipartUploadParts. Wildcards are accepted for this parameter.

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

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

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

Use this parameter to specify the bucket, folder, or object for which allow/deny permissions are set.

[-sid <SID>] - Statement Identifier

This optional parameter specifies a text comment for the object store server bucket policy statement. Alpha numeric characters are allowed as values for this parameter.

Examples

The following example creates an object store server bucket policy statement for Vserver vs1 and bucket1 which specifies allowed access to a readme folder for object store server user user1.

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

vserver object-store-server bucket policy statement delete

Delete a bucket policy statement

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

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

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

`-index <integer>` - Statement Index

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

Examples

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

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

vserver object-store-server bucket policy statement modify

Modify a bucket policy statement

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

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

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

-index <integer> - Statement Index

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

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

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

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

Use this parameter to specify resource operations. The set of resource operations object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads and ListMultipartUploadParts.

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

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

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

Use this parameter to specify the bucket, folder, or object for which allow/deny permissions are set.

[-sid <SID>] - Statement Identifier

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

Examples

The following example modifies an object store server bucket policy statement for Vserver vs1 and bucket1 which specifies allowed access to a readme folder for object store server user user1.

```
cluster1::> vserver object-store-server bucket policy statement modify
-vserver vs1 -bucket bucket1 -index 1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

vserver object-store-server bucket policy statement show

Show the bucket policy

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

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

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

[-index <integer>] - Statement Index

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

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

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

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

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

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

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

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

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

[-sid <SID>] - Statement Identifier

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

Examples

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

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

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

```
cluster1::> vserver object-store-server bucket policy show -vserver vs1
-bucket bucket1 -index 1
Vserver           :vs1
            Bucket            :bucket1
            Index             :1
            Effect            :allow
            Action            :GetObject
            Principal         :user-2
            Resource          :bucket1/readme/*
            Sid               :AllowAccessToUseruser1ForGetObject
```

vserver object-store-server group create

Create an Object Store Server Group

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-gid <integer>` - Group ID

This parameter specifies a unique ID used to identify a particular object store group.

-name <TextNoCase> - Group Name

This parameter specifies the name of the object store group.

-users <TextNoCase>,… - List of Users Belonging to the Group

Use this parameter to specify the list of object store users who belong to the object store group.

[-policies <TextNoCase>,…] - List of Policies Attached to the Group

Use this parameter to specify the list of object store policies that are attached to the object store group.

[-comment <text>] - Group Description

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

Examples

The following example creates an object store group named user_group for Vserver vs1:

```
cluster1::> vserver object-store-server group create -vserver vs1 -name
user_group -users user1,user2 -policies policy1,policy2 -comment
"UserGroup1"
```

vserver object-store-server group delete

Delete an Object Store Server Group

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

Description

The `vserver object-store-server group delete` command deletes an object store group.

Parameters

-vserver <Vserver Name> - Vserver Name

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

-gid <integer> - Group ID

This parameter specifies the ID of the object store group you want to delete.

Examples

The following example deletes an object store group for Vserver vs1:

```
cluster1::> vserver object-store-server group delete -vserver vs1 -gid 1
```

vserver object-store-server group modify

Modify an Object Store Server Group

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name
This parameter specifies the name of the Vserver for the object store group which you want to modify.

`-gid <integer>` - Group ID
This parameter specifies the ID of the object store group.

`[-name <TextNoCase>]` - Group Name
This parameter specifies the name of the object store group.

`[-users <TextNoCase>,…]` - List of Users Belonging to the Group
Use this parameter to specify the list of object store users who belong to the object store group.

`[-policies <TextNoCase>,…]` - List of Policies Attached to the Group
Use this parameter to specify the list of object store policies that are attached to the object store group.

`[-comment <text>]` - Group Description
This parameter specifies the text comment for the object store group.

Examples

The following example modifies the comment of the object store group for Vserver vs1:

```
cluster1::> vserver object-store-server group modify -vserver vs1 -gid 3
-comment "UserGroup"
```

vserver object-store-server group show

Display Object Store Server Groups

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

Description

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

Parameters

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

[-gid <integer>] - Group ID

If you specify this parameter, the command displays information on the object store server group that match the specified group ID.

[-name <TextNoCase>] - Group Name

If you specify this parameter, the command displays information on the object store server groups that match the specified group name.

[-users <TextNoCase>,…] - List of Users Belonging to the Group

If you specify this parameter, the command displays information on the object store server groups that match the specified user.

[-policies <TextNoCase>,…] - List of Policies Attached to the Group

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

[-comment <text>] - Group Description

If you specify this parameter, the command displays information on the object store server groups that match the specified comment.

Examples

The following example displays information for all object store groups in admin privilege:

```
cluster1::> vserver object-store-server group show
Vserver     Group ID  Group Name     Users            Policies
----------- --------- -------------- ---------------- --------------------
vs1                 3 UserGroup      user1, user2     policy1, policy2
   Comment: User_Privileges
vs1                 4 AdminGroup     admin1, admin2   policy1, policy2
   Comment: Admin_Privileges
    2 entries were displayed.
```

The following example displays information for a particular object store group associated with vserver vs1:

```
cluster1::> vserver object-store-server group show -vserver vs1 -gid 5
Vserver Name    :vs1
       Group ID        :5
       Group Name      :User-Group
       Users           :user_1, user_2
       Policies        :Policy1, Policy2, Policy3
       Comment         :User group
```

vserver object-store-server policy create

Create a policy

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-policy <TextNoCase>` - Policy Name

This parameter specifies the name of the object store policy.

`[-comment <text>]` - Comment

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

Examples

The following example creates an object store policy named Policy_1 for Vserver vs1:

```
cluster1::> vserver object-store-server policy create -vserver vs1 -policy
Policy_1 -comment "ReadAccessForBucket1"
```

vserver object-store-server policy delete

Delete a policy

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

Description

The `vserver object-store-server policy delete` command deletes an object store policy.

Parameters

`-vserver <Vserver Name>` - Vserver Name
This parameter specifies the name of the Vserver for the object store server you want to delete.

`-policy <TextNoCase>` - Policy Name
This parameter specifies the name of the object store policy you want to delete.

Examples

The following example deletes an object store policy for Vserver vs1:

```
cluster1::>vserver object-store-server policy delete -vserver vs1 -policy
Policy_2
```

vserver object-store-server policy modify

Modify a policy

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name
This parameter specifies the name of the Vserver for the object store policy you want to modify.

`-policy <TextNoCase>` - Policy Name
This parameter specifies the name of the object store policy.

`[-comment <text>]` - Comment
This parameter specifies the text comment for the object store policy.

Examples

The following example modifies the comment of the object store policy for Vserver vs1:

```
cluster1::> vserver object-store-server policy modify -policy Policy_1
-comment "Read_Access_for_Bucket2"
```

vserver object-store-server policy show

Show the policy

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

[-policy <TextNoCase>] - Policy Name

If you specify this parameter, the command displays information on the object store server policies that match the specified policy name.

[-is-read-only {true|false}] - Is Read-Only?

If you specify this parameter, the command displays information on the object store server policies that match the specified read only field.

[-comment <text>] - Comment

If you specify this parameter, the command displays information on the object store server policies that match the specified comment.

Examples

The following example displays information for all object store policies in admin privilege:

```
cluster1::> vserver object-store-server policy show
    Vserver     Name                Is Read-Only Comment
    ----------- ------------------- ------------ ----------------
    vs1         FullAccess          true         Read Only Policy: To allow
full access to S3 resources
    vs1         NoS3Access          true         Read Only Policy: To deny
access to all S3 resources
    vs1         Policy_1            false        Read_access_for_bucket1
    vs1         Policy_2            false        Read_access_for_bucket2
    vs1         ReadOnlyAccess      true         Read Only Policy: To allow
read-only access to S3 resources
    5 entries were displayed.
```

The following example displays information for a particular object store policy associated with Vserver vs1:

```
cluster1::> vserver object-store-server policy show -policy Policy_1
    Vserver     Name                Is Read-Only Comment
    ----------- ------------------- ------------ ----------------
    vs1         Policy_1            false        Read_access_for_bucket1
```

vserver object-store-server policy statement create

Create a Policy Statement

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-policy <TextNoCase>` - Policy Name

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

`-index <integer>` - Statement Index

This parameter specifies the unique index used to identify the particular object store server policy statement.

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

Use this parameter to specify whether or not access is allowed or denied when a user requests a specific action.

`-actions <Action>,…` - Policy Actions

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads and ListMultipartUploadParts. Wildcards are accepted for this parameter. If all operations needs to be specified, then use the wildcard character '*' to specify it.

`-resource <text>,…` - Buckets or Objects

Use this parameter to specify the bucket, folder, or object for which allow/deny permissions are set.

`[-sid <SID>]` - Statement Identifier

This optional parameter specifies a text comment for the object store server policy statement. This parameter name sid referred as statement identifier.

Examples

The following example creates an object store server policy statement for Vserver vs1 and Policy_1 which specifies allowed access to bucket1 resources.

```
cluster1::> vserver object-store-server policy statement create -vserver
vs1 -policy Policy_1 -effect allow  -actions
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,List
AllMyBuckets -resource bucket1/* -sid "FullAccesToBucket1"
```

vserver object-store-server policy statement delete

Delete a Policy Statement

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

This parameter specifies the name of the Vserver whose policy statement you want to delete.

`-policy <TextNoCase>` - Policy Name

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

`-index <integer>` - Statement Index

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

Examples

The following example deletes an object store server policy statement with index 1 of Vserver vs1 and policy Policy_1.

```
cluster1::> vserver object-store-server policy statement delete -vserver
vs1 -policy Policy_1 -index 1
```

vserver object-store-server policy statement modify

Modify a Policy Statement

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-policy <TextNoCase>` - Policy Name

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

`-index <integer>` - Statement Index

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

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

Use this parameter to specify whether or not access is allowed or denied when a user requests a specific action.

`[-actions <Action>,…]` - Policy Actions

Use this parameter to specify resource operations. The set of resource operations object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads and ListMultipartUploadParts.

`[-resource <text>,…]` - Buckets or Objects

Use this parameter to specify the bucket, folder, or object for which allow/deny permissions are set.

`[-sid <SID>]` - Statement Identifier

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

Examples

The following example modifies an object store server policy statement for Vserver vs1 and Policy_1 which specifies allowed access to bucket1 resources.

```
cluster1::> vserver object-store-server policy statement modify -vserver
vs1 -policy Policy_1 -index 5 -effect allow -actions
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,List
AllMyBuckets -resource bucket1/* -sid FullAccesToBucket1Resources
```

vserver object-store-server policy statement show

Show Policy Statements

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

[-policy <TextNoCase>] - Policy Name

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

[-index <integer>] - Statement Index

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

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

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

[-actions <Action>,…] - Policy Actions

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

[-resource <text>,…] - Buckets or Objects

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

[-sid <SID>] - Statement Identifier

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

Examples

The following example displays information on object store server policy statements for Vserver vs1 and policy Policy_1:

```
cluster1::> vserver object-store-server policy statement show -vserver vs1
-policy Policy_1
Vserver   Policy       Index  Effect Actions          Resources
--------- ------------ ------ ------ ---------------- -----------------
vs1
          Policy_1          1 allow  ListBucket       *
          Policy_1          5 allow  GetObject,       bucket1/*
                                     PutObject,
                                     DeleteObject,
                                     ListBucket,
                                     GetBucketAcl,
                                     GetObjectAcl,
                                     ListAllMyBuckets
   Sid: FullAccesToBucket1
2 entries were displayed.
```

The following example displays detailed information of the object store server policy statement associated with Vserver vs1 and policy Policy_1:

```
cluster1::> vserver object-store-server policy statement show -vserver vs1
-policy Policy_1 -index 5
Vserver: vs1
      Policy: Policy_1
       Index: 5
      Effect: allow
     Actions: GetObject, PutObject, DeleteObject, ListBucket,
GetBucketAcl, GetObjectAcl, ListAllMyBuckets
    Resource: bucket1/*
         Sid: FullAccesToBucket1
```

vserver object-store-server user create

Create an object store server user

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

Description

The `vserver object-store-server user create` command creates an object store user. This will generate an access-key and a secret-key to be used for aws v4 authentication

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-user <TextNoCase>` - Object Store Server User Name

This parameter specifies the name of the object store user.

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

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

Examples

The following example creates an object store user user1 for Vserver vs1.

```
cluster1::> vserver object-store-server user create -vserver vs1 -user
user1
```

vserver object-store-server user delete

Delete an object store server user

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

Description

The `vserver object-store-server user delete` command deletes an object store user.

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-user <TextNoCase>` - Object Store Server User Name

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

Examples

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

```
cluster1::> vserver object-store-server user delete -vserver vs1 -user
user1
```

vserver object-store-server user modify

Modify an object store server user

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

Description

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

Parameters

`-vserver <Vserver Name>` - Vserver Name

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

`-user <TextNoCase>` - Object Store Server User Name

This parameter specifies the name of the object store user.

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

This parameter specifies the text comment for the object store user.

Examples

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

```
cluster1::> vserver object-store-server user modify -vserver vs1 -user
user1 -comment testuser
```

vserver object-store-server user regenerate-keys

Regenerate keys for object store user

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

Description

The `vserver object-store-server user regenerate-keys` command regenerates a new access-key and secret-key for an object store user

Parameters

`-vserver <Vserver Name>` - Vserver Name

This parameter specifies the name of the Vserver on which the keys should be generated for the object store user. The object store user must already exist.

`-user <TextNoCase>` - Object Store Server User Name

This parameter specifies the name of the object store user.

Examples

The following example regenerates the keys for object store user for Vserver vs1.

```
cluster1::> vserver object-store-server user regenerate-keys -vserver vs1
-user user1
```

vserver object-store-server user show

Display object store server users

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

Description

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

Parameters

{ [-fields <fieldname>,…]

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

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver Name

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

[-user <TextNoCase>] - Object Store Server User Name

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

[-id <integer>] - Object Store Server User ID

If you specify this parameter, the command displays information only for object store users that match the specified user id.

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

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

[-access-key <text>] - Access Key for the Object Store Server User

If you specify this parameter, the command displays information only for object store users that match the specified access key.

[-secret-key <text>] - Secret Key for the Object Store Server User (privilege: advanced)

If you specify this parameter, the command displays information only for object store users that match the specified secret key. This parameter is available only in advanced privilege mode.

Examples

The following example displays information of all object store users in admin privilege:

```
cluster1::> vserver object-store-server user show
Vserver     User            ID        Access Key          Secret Key
----------- --------------- --------- -------------------
-------------------
vs1         user1           1
Fb4k9g049au0au22d0wpX7GGQ3SLayvlOCcA0ycDAPlPa95YRA8N7lzZN_69SZ77_bQ909ur9m
Iehz5_Jcb4VjdW9BlTXj4D5621k4_ghaiD3uEbF9_c5Q0oD7TBvx83
   Comment: testuser
vs1         user2           2
QO2PPR_U00Y9u4qsjpK49egAs2yJ_0iZQcXPuVumpI6ybn0ca4TY7vXO8N5__072cXzTn_hU6j
W9ER7bja_GDcH3D3g2w9XVB_d_S3wdd3DgI_DBZgb_YNRI9Ae_Cy34
2 entries were displayed.
```

The following example displays information of a particular object store user associated with Vserver vs1:

```
cluster1::> vserver object-store-server user show -vserver vs1 -user user1
                              Vserver Name: vs1
              Object Store Server User Name: user1
                Object Store Server User ID: 1
       Object Store Server User Description: testuser
Access Key for the Object Store Server User:
Fb4k9g049au0au22d0wpX7GGQ3SLayvlOCcA0ycDAPlPa95YRA8N7lzZN_69SZ77_bQ909ur9m
Iehz5_Jcb4VjdW9BlTXj4D5621k4_ghaiD3uEbF9_c5Q0oD7TBvx83
```

The following example displays information of all object store users in advanced privilege:

```
cluster1::*> vserver object-store-server user show
Vserver     User            ID        Access Key          Secret Key
----------- --------------- --------- -------------------
-------------------
vs1         user1           1
Fb4k9g049au0au22d0wpX7GGQ3SLayvlOCcA0ycDAPlPa95YRA8N7lzZN_69SZ77_bQ909ur9m
Iehz5_Jcb4VjdW9BlTXj4D5621k4_ghaiD3uEbF9_c5Q0oD7TBvx83

6SN5oxyz92sw1P5yc2_BH9XHnAi3XgP9Cx876NGlh5382222kL5Z92Jx2qcV795ZkwyjsBt65D
j804p64__h8D30XqY_d5kbr3jt9V_S79s1AnCB8gD2f9hKl2sbn3y3
   Comment: testuser
vs1         user2           2
QO2PPR_U00Y9u4qsjpK49egAs2yJ_0iZQcXPuVumpI6ybn0ca4TY7vXO8N5__072cXzTn_hU6j
W9ER7bja_GDcH3D3g2w9XVB_d_S3wdd3DgI_DBZgb_YNRI9Ae_Cy34

nQB2tQ1_Og_a6c0q2r4sOtK1rM9Ch9qA4arJJ8f52_n4cQWmZGrcxBWYnbIr573rb2rqPu43tm
tD8BSjD9_s2Y5C_8hx1BNXM99r494p_1hzYa_Rd1Ij9S68APlCtJo0
2 entries were displayed.
```

The following example displays information of a particular object store user associated with Vserver vs1 in advanced privilege:

```
cluster1::*> vserver object-store-server user show -vserver vs1 -user
user1
                              Vserver Name: vs1
              Object Store Server User Name: user1
                Object Store Server User ID: 1
       Object Store Server User Description: testuser
Access Key for the Object Store Server User:
Fb4k9g049au0au22d0wpX7GGQ3SLayvlOCcA0ycDAPlPa95YRA8N7lzZN_69SZ77_bQ909ur9m
Iehz5_Jcb4VjdW9BlTXj4D5621k4_ghaiD3uEbF9_c5Q0oD7TBvx83
Secret Key for the Object Store Server User:
6SN5oxyz92sw1P5yc2_BH9XHnAi3XgP9Cx876NGlh5382222kL5Z92Jx2qcV795ZkwyjsBt65D
j804p64__h8D30XqY_d5kbr3jt9V_S79s1AnCB8gD2f9hKl2sbn3y3
```

vserver peer commands

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 <vserver>` - Peer Vserver Name

Specifies name of the peer Vserver with which the Vserver peer relationship was initiated.

`[-local-name <vserver>]` - Peer Vserver Local Name

Specifies the unique local name to identify the peer Vserver with which the Vserver peer relationship was initiated. The default value is the remote peer Vserver name.

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
```

The following example illustrates how to accept the Vserver peer relationship between Vservers *`pvs1.example.com`* residing on *`cluster2`* , and *`pvs1.example.com`* residing on *`cluster1`* . During execution of vserver peer create command on peer cluster, peer Vserver name is locally refered by unique system generated name *`pvs1.example.com.1`* . Using `vserver peer accept` command specify the unique `-local-name` for peer Vserver.

```
cluster2::> vserver peer accept -vserver pvs1.example.com -peer-vserver
pvs1.example.com.1 -local-name locallyUniqueName
```

Related Links

- vserver peer create

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 the peer cluster.

Parameters

`-vserver <vserver>` - Vserver Name

Specifies the name of the local Vserver.

`-peer-vserver <vserver>` - 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|file-copy|lun-copy|flexcache}` - Peering Applications

Specifies the applications for which the Vserver peer relationship is created.

`[-local-name <vserver>]` - Peer Vserver Local Name

Specifies the unique local name to identify the peer Vserver with which you want to create the Vserver peer relationship. The default value is the remote peer Vserver name.

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
```

The following example illustrates how to create an intercluster Vserver peer relationship between Vserver *`lvs1.example.com`* , residing on *`cluster1`* , and *`lvs1.example.com`* , residing on *`cluster2`* . The relationship is created for SnapMirror. The `-local-name` parameter is specified to create a local name used to identify the peer Vserver in cases where the name of the peer Vserver name is not uniquely referenced from local cluster.

```
cluster1::> vserver peer create -vserver lvs1.example.com -peer-vserver
lvs1.example.com -peer-cluster cluster2 -applications snapmirror -local
-name cluster2lvs1locallyUniqueName

cluster1::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
lvs1.example.com
            cluster2lvs1locallyUniqueName
                        initiated    cluster2          snapmirror
lvs1.example.com
cluster1::> vserver peer show -instance
Local Vserver Name: lvs1.example.com
   Peer Vserver Name: cluster2lvs1locallyUniqueName
       Peering State: initiated
Peering Applications: snapmirror
 Remote Vserver Name: lvs1.example.com
```

The following example illustrates how to create an intercluster Vserver peer relationship between Vserver *lvs1* , residing on *cluster1* , and Vserver *pvs1* , residing on *cluster2* . The relationship is created for SnapMirror. The following Vserver peer permission exists on remote cluster *cluster2* for local Vserver *pvs1* .

```
cluster2::> vserver peer permission show
Peer Cluster     Vserver         Applications
---------------- --------------- -----------------
cluster1         pvs1            snapmirror
1 entries were displayed.

cluster1::> vserver peer create -vserver lvs1 -peer-vserver pvs1 -peer
-cluster cluster2 -applications snapmirror

cluster1::> vserver peer show
            Peer        Peer                          Peering
Remote
Vserver     Vserver     State        Peer Cluster     Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
lvs1        pvs1        peered       cluster2          snapmirror     pvs1

cluster2::> vserver peer show
            Peer        Peer                          Peering
Remote
Vserver     Vserver     State        Peer Cluster     Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        lvs1        peered       cluster1          snapmirror     lvs1
```

Here is an another example which creates an intracluster Vserver peer relationship.

```
cluster1::> vserver peer create -vserver lvs1.example.com -peer-vserver
lvs2.example.com -applications snapmirror
```

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.

Parameters

-vserver <vserver> - Vserver Name

Specifies the local Vserver name for which you want to delete the Vserver peer relationship.

-peer-vserver <vserver> - 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.

[-foreground {true|false}] - Foreground

This parameter optionally specifies whether the Vserver peer delete operation can be executed in the background. If nothing is specified, by default the Vserver peer delete operation is executed in the background.

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
```

vserver peer modify-local-name

Modify the local name for a peer Vserver

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

Description

The `vserver peer modify-local-name` command modifies the local name for a remote peer Vserver. The new local name must be unique.

Parameters

-peer-cluster <text> - Peer Cluster

Use this parameter to specify the peer cluster.

-peer-vserver <text> - Remote Peer Vserver

Use this parameter to specify the existing remote peer Vserver name.

-new-name <vserver> - Remote Peer Vserver Local Name

Use this parameter to specify the new local name of the peer Vserver. The new local name must conform to the same rules as a Vserver name.

Examples

```
cluster2::> vserver peer modify-local-name -peer-cluster cluster1 -peer
-vserver vs51.example.com -new-name vs51_cluster1.example.com
```

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 <vserver>` - Peer Vserver Name

Specifies name of the peer Vserver for which you want to modify applications of the Vserver peer relationship.

`-applications {snapmirror|file-copy|lun-copy|flexcache}` - 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
```

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 <vserver> - 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
```

vserver peer repair-peer-name

Repair the peer vserver name that was not updated during the last rename operation

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

Description

Updates the peer Vserver name in remote peer clusters for the specified Vserver in the local cluster.

Parameters

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

Name of the Vserver in the local cluster. This name will be repaired on remote peer clusters.

Examples

The following example updates the peer-Vserver name across the peered clusters:

```
cluster1::*> vserver peer repair-peer-name -vserver vs1.example.com
Info: Command completed successfully
```

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 <vserver>` - 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
```

vserver peer show-all

(DEPRECATED)-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
- Local Vserver UUID
- Peer Vserver UUID
- Peer cluster name
- Applications
- State of the peering relationship
- Remote 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>] - 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.

[-vserver-uuid <UUID>] - Local Vserver UUID (privilege: advanced)

If this parameter is specified, the command displays relationships that match the specified local Vserver UUID.

[-peer-vserver-uuid <UUID>] - Peer Vserver UUID (privilege: advanced)

If this parameter is specified, the command displays relationships that match the specified peer Vserver UUID.

[-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|file-copy|lun-copy|flexcache}] - 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.

[-remote-vserver-name <text>] - Remote Vserver Name

If this parameter is specified, the command displays relationships that match the specified remote Vserver.

Examples

The following example illustrates how to display Vserver peer relationships. +

```
cluster1::> vserver peer show-all
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
lvs1.example.com
            lvs2.example.com
                        peered       cluster1          snapmirror
lvs2.example.com
lvs1.example.com
            pvs1.example.com
                        peered       cluster2          snapmirror
pvs1.example.com
lvs2.example.com
            lvs1.example.com
                        peered       cluster1          snapmirror
lvs1.example.com
lvs3.example.com
            pvs1_cluster3.example.com
                        peered       cluster3          snapmirror
pvs1.example.com
lvs1.example.com
            lvs1_cluster4.example.com
                        peered       cluster4          snapmirror
lvs1.example.com
5 entries were displayed.
```

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
- Local Vserver UUID
- Peer Vserver UUID
- Peer cluster name
- State of the peering relationship

- Applications
- Remote 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>] - 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|file-copy|lun-copy|flexcache}] - 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.

[-peer-vserver-uuid <UUID>] - Peer Vserver UUID (privilege: advanced)

If this parameter is specified, the command displays relationships that match the specified peer Vserver UUID.

[-vserver-uuid <UUID>] - Local Vserver UUID (privilege: advanced)

If this parameter is specified, the command displays relationships that match the specified local Vserver UUID.

[-remote-vserver-name <text>] - Remote Vserver Name

If this parameter is specified, the command displays relationships that match the specified remote Vserver.

Examples

The following examples illustrate how to display Vserver peer relationships. + Cluster administrator:

```
cluster1::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
lvs1.example.com
            lvs2.example.com
                        peered       cluster1          snapmirror
lvs2.example.com
lvs1.example.com
            pvs1.example.com
                        peered       cluster2          snapmirror
pvs1.example.com
lvs2.example.com
            lvs1.example.com
                        peered       cluster1          snapmirror
lvs1.example.com
lvs3.example.com
            pvs1_cluster3.example.com
                        peered       cluster3          snapmirror
pvs1.example.com
lvs1.example.com
            lvs1_cluster4.example.com
                        peered       cluster4          snapmirror
lvs1.example.com
5 entries were displayed.
```

Vserver administrator:

```
vs11.example.com::> vserver peer show
            Peer        Peer         Peering               Remote
Vserver     Vserver     State        Applications          Vserver
----------- ----------- ------------ --------------------- ----------
vs11.example.com
            pvs21.example.com
                        peered       snapmirror
pvs21.example.com
vs11.example.com
            vs12.example.com
                        peered       file-copy, snapmirror
vs12.example.com
2 entries were displayed.
```

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 <vserver>` - 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
```

vserver peer permission create

Create a new Vserver peer permission

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

Description

The `vserver peer permission create` command creates a new Vserver peer permission that can be used during intercluster Vserver peer relationship creation. Once this permission exists for a local Vserver and peer cluster combination on local cluster, no explict vserver peer accept command is required for any incoming Vserver peer relationship creation request from a remote cluster for that local Vserver. Peer relationship directly changes state to *`peered`* on both clusters.

Parameters

`-peer-cluster <text>` - Peer Cluster Name

Specifies the name of the peer Cluster.

-vserver <text> - Vserver Name

Specifies the name of the local Vserver. Use "*" to create permission that applies for all local Vservers.

-applications {snapmirror|flexcache} - Peering Applications

Specifies the applications that can make use of the intercluster Vserver peer relationship.

Examples

The following example illustrates how to create Vserver peer permissions:

```
cluster1::> vserver peer permission create -peer-cluster cluster2 -vserver
vs1 -applications snapmirror

The following example illustrates how to create a Vserver peer permission
that applies for all the local Vservers

cluster1::> vserver peer permission create -peer-cluster cluster2 -vserver
"*" -applications snapmirror

Warning: This Vserver peer permission applies to all local Vservers. After
that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
cluster1::> vserver peer permission show
Peer Cluster     Vserver         Applications
---------------- --------------- -----------------
cluster2         "*"             snapmirror
cluster2         vs1             snapmirror
2 entries were displayed.

Note that both  all  Vservers and any local Vserver name permission can
exists at same
time.
```

Related Links

- vserver peer accept

vserver peer permission delete

Delete a Vserver peer permission

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

Description

The `vserver peer permission delete` command deletes Vserver peer permissions.

Parameters

`-peer-cluster <text>` - Peer Cluster Name

Specifies the name of the peer Cluster.

`-vserver <text>` - Vserver Name

Specifies the name of the local Vserver.

Examples

The following example illustrates how to delete Vserver peer permissions:

```
cluster1::> vserver peer permission delete -peer-cluster cluster2 -vserver
vs1
```

vserver peer permission modify

Modify the Existing Vserver peer permission

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

Description

The `vserver peer permission modify` command is used to modify attributes of the Vserver peer permission relationship. Changes made using this command will only apply to Vserver peer relationships that are created after the Vserver peer permission have been modified. Vserver peer permission is used to give permission to a local Vserver for intercluster Vserver peer relationship creation so that the command vserver peer accept is not required for incoming Vserver peer relationship creation from a remote cluster for that local Vserver.

Parameters

`-peer-cluster <text>` - Peer Cluster Name

Specifies the name of the peer cluster.

`-vserver <text>` - Vserver Name

Specifies name of the local Vserver for which you want to modify applications of the Vserver peer permission relationship.

`-applications {snapmirror|flexcache}` - Peering Applications

Specifies the applications that can make use of the intercluster Vserver peer relationship.

Examples

The following example illustrates how to modify Vserver peer permissions:

```
cluster1::*> vserver peer permission modify -peer-cluster cluster2
-vserver vs1 -applications snapmirror
```

Related Links

- vserver peer accept

vserver peer permission show

Display Vserver peer permissions

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

Description

The `vserver peer permission show` command displays the following information about Vserver peer permissions:

- Peer cluster name
- Local Vserver name
- Applications

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.

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

If this parameter is specified, the command displays permissions that have the specified peer cluster name.

[-vserver <text>] - Vserver Name

If this parameter is specified, the command displays permissions that match the specified local Vserver.

[-applications {snapmirror|flexcache}] - Peering Applications

If this parameter is specified, the command displays permissions that have the specified applications.

Examples

The following examples illustrate how to display Vserver peer permissions:

```
cluster1::> vserver peer permission show
Peer Cluster     Vserver         Applications
---------------- --------------- -----------------
cluster2         "*"             snapmirror
cluster3         vs1             snapmirror
2 entries were displayed.
```

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.

`[-local-lifs <lif-name>,…]` - List of Local LIFs

List of LIFs to be used for this peering relationship. The LIF role can be data or node-mgmt or intercluster or cluster-mgmt.

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 and list of local LIFs *`lif1, lif2`* to be used.

```
Cluster1::> vserver peer transition create -local-vserver vs1.example.com
-src-filer-name src1.example.com -multi-path-address src1-e0d.example.com
-local-lifs lif1,lif2
```

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 -local-vserver lvs1.example.com
-src-filer-name src1.example.com
```

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 is used to modify the multipath address or local LIFs 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.

`[-local-lifs <lif-name>,…]` - List of Local LIFs

List of LIFs to be used for this peering relationship. The LIF role can be data or node-mgmt or intercluster or cluster-mgmt.

Examples

The following example illustrates how to modify a transition peer relationship`s multipath address.

```
cluster1::> vserver peer transition modify -local-vserver vs1.example.com
-src-filer-name src1.example.com -multi-path-address src1-e0b.example.com
```

The following example illustrates how to modify the local LIFs of a transition peer relationship.

```
Cluster1::> vserver peer transition modify -local-vserver vs1.example.com
-src-filer-name src1.example.com
-local-lifs lif1,lif2
```

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
- Local 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.

[-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.

[-local-lifs <lif-name>,…] - List of Local LIFs

If this parameter is specified, the command displays information about the specified local LIFs.

Examples

```
cluster1::> vserver peer transition show
Vserver  Source Filer  Multi Path Address    Local LIFs
-------  ------------  -----------------     ----------------
vs1.example.com                              lif1, lif2
          src1.example.com
                        src1-e0b.example.com
```

vserver san commands

vserver san prepare-to-downgrade

Restore the SAN Configurations to Earlier Release of Data ONTAP Version.

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

Description

This command initiates the procedure to restore the configuration to Earlier Release of Data ONTAP Version.

As part of this command, capability for making SAN LIF offline if placed on the DR auxiliary partner as part of LIF placement in Metrocluster environment will be disabled.

Parameters

-feature-set <ClusterVersion> - Disable the capability introduced in the Data ONTAP Version

Specifies the DATA ONTAP Cluster Version from revert to.

Examples

```
cluster1::> vserver san prepare-to-downgrade -feature-set 8.3.1
```

Clears the SAN configuration to make it compatible to an earlier DATA ONTAP release.

vserver security commands

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.

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.

Parameters

`-vserver <vserver name>` - 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.

`[-ignore-broken-symlinks {true|false}]` - Skip Broken Symlinks (privilege: advanced)

If you specify this parameter as *`true`* , the file-directory apply job will skip all the symlinks that are broken instead of failing the job.

Examples

The following example applies a security policy named “p1” to Vserver vs0.

```
cluster1::> vserver security file-directory apply -vserver vs0 -policy
-name p1
```

vserver security file-directory remove-slag

Removes Storage-Level Access Guard

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

Description

The `vserver security file-directory remove-slag` command removes Storage-Level Access Guard (SLAG) security from the specified volume or qtree path.

Parameters

`-vserver <vserver>` - Vserver

Specifies the name of the Vserver that is associated with the volume or qtree path from where you want to remove SLAG.

`-path <text>` - Path

Specifies the volume or qtree mounted junction path from which you want to remove SLAG security.

Examples

The following example removes SLAG security from the volume path "/vol1" on Vserver vs1.

```
cluster1::>vserver security file-directory show -vserver vs1 -path /vol1
Vserver: vs1
                    File Path: /vol1
            Security Style: mixed
           Effective Style: unix
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 755
     Unix Mode Bits in Text: rwxr-xr-x
                       ACLs: Storage-Level Access Guard security
DACL (Applies to Directories):
                                ALLOW-CIFS1\Administrator-0x1200a9
                              DACL (Applies to Files):
                                ALLOW-CIFS1\Administrator-0x1200a9
cluster1::>vserver security file-directory remove-slag -path /vol1
-vserver vs1
cluster1::>vserver security file-directory show -vserver vs1 -path /vol1
                     Vserver: vs1
                    File Path: /vol1
            Security Style: mixed
           Effective Style: unix
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 755
     Unix Mode Bits in Text: rwxr-xr-x
                       ACLs: -
```

The following example removes SLAG security from the qtree path "/vol1/q1" on Vserver vs1.

```
cluster1::>vserver security file-directory show -vserver vs1 -path
/vol1/q1
Vserver: vs1
                     File Path: /vol1/q1
                 Security Style: mixed
                Effective Style: unix
                 DOS Attributes: 10
         DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
                   Unix User Id: 0
                  Unix Group Id: 0
                 Unix Mode Bits: 755
         Unix Mode Bits in Text: rwxr-xr-x
                           ACLs: Storage-Level Access Guard security
DACL (Applies to Directories):
                                    ALLOW-CIFS1\Administrator-0x1200a9
                                 DACL (Applies to Files):
                                    ALLOW-CIFS1\Administrator-0x1200a9
cluster1::>vserver security file-directory remove-slag -path /vol1/q1
-vserver vs1
cluster1::>vserver security file-directory show -vserver vs1 -path
/vol1/q1
                       Vserver: vs1
                     File Path: /vol1/q1
                 Security Style: mixed
                Effective Style: unix
                 DOS Attributes: 10
         DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
                   Unix User Id: 0
                  Unix Group Id: 0
                 Unix Mode Bits: 755
         Unix Mode Bits in Text: rwxr-xr-x
                           ACLs: -
```

vserver security file-directory show-effective-permissions

Display effective file or folder permissions

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

Description

The `vserver security file-directory show-effective-permissions ` command displays the effective permission granted to a Windows or UNIX user on the specified file or folder path. The command output depends on the parameter or parameters specified with the command.

The `-vserver` , `-win-user-name` or `-unix-user-name` and `-path` parameters are required for this command. If the optional parameter `-share-name` is specified, it will display the effective share permission.

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

Use this required parameter to specify the Vserver that contains the path to the file or folder specified with the required `-path` parameter. Query characters, such as "*", are not supported.

{ -win-user-name <text> - Windows User Name

Use this parameter to specify the Windows user for which effective permission needs to be displayed on the given file or folder.

| -unix-user-name <text> - Unix User Name }

Use this parameter to specify the UNIX user for which effective permission needs to be displayed on the given file or folder.

-path <text> - File Path

Use this mandatory parameter to specify the path of the file or the folder for which you want to display effective permissions. The path is relative to the Vserver root volume. If `-share-name` is specified then the path will be relative to the share path. Query characters,such as "*", are not supported.

[-share-name <Share>] - CIFS Share Name

If you specify this optional parameter, the command displays the file or directory effective permission for the mentioned user, only for files and directories con-tained 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 the default. If this optional parameter is specified, then it will also display the effective share permission of the user. Wildcard query characters are not supported.

[-client-ip-address <IP Address>] - Client IP Address

If you specify this optional parameter, the command displays the effective permission for the user with the specified client ip address.

[-expand-mask {true|false}] - Expand Bit Masks

If you specify this optional parameter, the command displays effective permission for files and directories where the hexadecimal bit mask entries are in expanded bit form. If set to default (false), the command displays effective permission for file or directory in collapsed (textual) form.

[-share-path <text>] - CIFS Share Path

If you specify this parameter, the command displays information only about the CIFS share that match the specified path. Query characters, such as "*", are not supported.

[-permission <Security acl>,…] - Effective Permissions

If you specify this parameter, the command displays effective permission only if specified permission matches. Wildcard query characters are not supported.

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 `vserver security 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.

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 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. If the path's last subcomponent has a wildcard ("*"), the output will display information for all files and directories below the parent path.

If you want to display information of a file or directory which contains wildcard ("*") as its last sub-component, then provide the complete path inside "<path>".

For instance, vserver security file-directory show -vserver vs1 -path "/vol1/**" will show ACL information for the directory named ""**, only.

| [-inode <integer>] - File Inode Number }

Use this field to specify the inode number of the file or folder for which you want to display security information. If the volume name is not specified, inode is searched in 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 you specify this parameter, 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 you specify this parameter, 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 directory security for files and directories where the hexadecimal bit mask entries are in collapsed form.

| [-textual-mask {true|false}] - Show Textual Mask

If you specify this parameter as *true* , the command displays information about file and directory security for files and directories where the hexadecimal bit mask is translated to texual format.

| [-sddl {true|false}] - Display ACLs in SDDL Format }

If you specify this parameter, the command displays the ACL information for files and directories in Security Descriptor Definition Language (SDDL) format. If the file has `effective-style` as "unix" then this flag has no effect.

[-security-style <security style>] - 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.

[-effective-style <security style>] - 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.

[-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. If the specified path is a volume or qtree path and Storage-Level Access Guard (SLAG) is configured on the volume or qtree, this parameter displays the SLAG information. It also displays the Dynamic Access Control (DAC) policies if DAC is configured for the given file or directory path. 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.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol4
              (vserver security file-directory show)
Vserver: vs1
                           File Path: /vol4
                 File Inode Number: 64
                    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.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/a/b/file.txt -volume-name vol1
                  (vserver security file-directory show)
Vserver: vs1
                                File Path: /vol1/a/b/file.txt
                      File Inode Number: 101
                         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 of the volume path "/vol1" containing SLAG.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                 File Inode Number: 64
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                       POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
                                       ALLOW CALLBACK-DAC\skanyal-
0x1200a9-OI|CI

((@User.department==@Resource.Department_MS@Resource.Impact_MS>1000)@Devic
e.department==@Resource.Department_MS)
Storage-Level Access Guard security
                                    SACL (Applies to Directories):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Directories):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
                                    SACL (Applies to Files):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Files):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
```

The following example displays the security information of the qtree path "/vol1/q1" containing SLAG.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/vol1/q1
                           Vserver: vs1
                         File Path: /vol1/q1
                 File Inode Number: 105
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
Storage-Level Access Guard security
                                    SACL (Applies to Directories):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Directories):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
                                    SACL (Applies to Files):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Files):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
```

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 abthe file-directory security job.

```
cluster1::> vserver security file-directory apply -policy-name pol
-vserver vs1
cluster1::> 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.

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.

Parameters

`-vserver <vserver name>` - 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.

Every newly created security descriptor contains the 4 default DACL ACEs as mentioned below:

```
Vserver: vserver1
                          NTFS Security Descriptor Name: sd1
Account Name     Access   Access             Apply To
                                            Type     Rights
                           --------------   -------  -------
-----------
                           BUILTIN\Administrators
                                            allow    full-control
this-folder, sub-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-folders, files
```

+

`[-owner <name or sid>]` - Owner

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

> 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. The value for the user name is ignored for Storage-Level Access Guard (SLAG).

`[-group <name or sid>]` - Primary Group (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

> 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. The value for the user name is ignored for SLAG.

`[-control-flags-raw <Hex Integer>]` - Raw Control Flags (privilege: advanced)

Specifies the control flags in the security descriptor.

> The value for the control flag is ignored for SLAG.

Examples

The following example creates an NTFS security descriptor named “sd1” on Vserver "vs1" and assigns “DOMAIN\Administrator” as the security descriptor owner.

```
cluster1::> vserver security file-directory ntfs create -ntfs-sd sd1
-vserver vs1 -owner DOMAIN\Administrator
cluster1::> vserver security file-directory ntfs show -vserver vs1 -ntfs
-sd sd1
                                        Vserver: vs1
                      Security Descriptor Name: sd2
                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).

Parameters

`-vserver <vserver name>` - 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.

```
cluster1::> 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` of the security descriptor with this command.

Parameters

`-vserver <vserver name>` - 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

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

> 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. The value for the user name is ignored for Storage-Level Access Guard (SLAG).

`[-group <name or sid>]` - Primary Group (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

> 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. The value for the user name is ignored for SLAG.

`[-control-flags-raw <Hex Integer>]` - Raw Control Flags (privilege: advanced)

Specifies the control flags in the security descriptor to be modified.

> The value for the control flag is ignored for SLAG.

Examples

The following example modifies the owner of an NTFS security descriptor named "sd2" on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs modify -ntfs-sd sd2
-vserver vs1 -owner domain\administrator
cluster1::> 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 security 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.

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 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

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 (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.

```
cluster1::> 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 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.

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.

Parameters

`-vserver <vserver name>` - 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

> 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` 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` 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

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task`.

Examples

The following example adds a DACL entry to the security descriptor named “sd1” on Vserver "vs1" for the "DOMAIN\Administrator" account.

```
cluster1::> 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
cluster1::> 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
- -apply-to

Parameters

`-vserver <vserver name>` - 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

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` 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

| [-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.

| [-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` 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

[-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

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task`.

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.

```
cluster1::> 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
cluster1::> 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

Parameters

`-vserver <vserver name>` - 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.

```
cluster1::> 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.

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 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

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

[-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.

[-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

[-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.

```
cluster1::> vserver security file-directory ntfs dacl show
Vserver: vs1
                NTFS Security Descriptor Name: sd2
Account Name     Access   Access             Apply To
                                  Type     Rights
                  --------------   -------  -------            -----------
                  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-folders, files
              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.

> 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.

Parameters

`-vserver <vserver name>` - 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}` - Success or Failure

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

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 rights that you want to get audited for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` 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 get audited for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` 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 get audited 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

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task .`

Examples

The following example adds a SACL entry to the security descriptor named “sd1” on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs sacl add -ntfs-sd sd1
-access-type failure -account DOMAIN\Administrator -rights full-control
-apply-to this-folder -vserver vs1
cluster1::> vserver security file-directory ntfs sacl 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

Parameters

`-vserver <vserver name>` - 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} - Success or Failure

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

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 rights that you want to get audited for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` 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

| [-rights-raw <Hex Integer>] - Raw Access Rights (privilege: advanced)

Specifies the raw rights that you want to get audited 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.

| [-advanced-rights <Advanced access right>,…] - Advanced Access Rights }

Specifies the advanced rights that you want to get audited for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` 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

[-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

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task`.

Examples

The following example modifies the rights and -apply-to fields in the SACL entry.

```
cluster1::> vserver security file-directory ntfs sacl modify -ntfs-sd sd2
-access-type success -account BUILTIN\Administrators -vserver vs1 -rights
modify -apply-to this-folder,sub-folders
cluster1::> vserver security file-directory ntfs sacl 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 sacl 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 sacl 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

Parameters

`-vserver <vserver name>` - 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}` - Success or Failure

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.

```
cluster1::> vserver security file-directory ntfs sacl remove -ntfs-sd sd2
-access-type success -account BUILTIN\Administrators -vserver vs1
```

vserver security file-directory ntfs sacl 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 sacl 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.

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 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}] - Success or Failure

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

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

[-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.

[-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

[-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.

```
cluster1::> vserver security file-directory sacl show
               (vserver security file-directory ntfs sacl show)
Vserver: vs1
                 NTFS Security Descriptor Name: sd1
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.

> 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.

> 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.

Parameters

`-vserver <vserver name>` - 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.

```
cluster1::> vserver security file-directory policy create -policy-name
policy1 -vserver vs1
            cluster1::> 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.
```

Deleting a policy fails if a job is currently running for the specified policy.

Parameters

-vserver <vserver name> - 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.

```
cluster1::> 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.

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 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.

```
cluster1::> 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.

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.

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.

Adding a policy task fails if a job is currently running for the specified policy to which a task is being added.

- Apply a policy to the associated Vserver.

Parameters

`-vserver <vserver name>` - 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.

`[-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.

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.

[-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”.

> 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

> The ntfs-mode value is ignored for Storage-Level Access Guard (SLAG).

[-ntfs-sd <ntfs sd name>,…] - NTFS Security Descriptor Name

Specifies the list of security descriptor names to apply to the path specified in the `-path` parameter.

[-access-control {file-directory|slag}] - Access Control Level

Specifies the access control of the task to be applied. Valid values are *`file-directory`* or *`slag`* . Use the value *`slag`* to apply the specified security descriptors with the task for the volume or qtree. Otherwise, the security descriptors are applied on files and directories at the specified path. The value *`slag`* is not supported on FlexGroups. The default value is *`file-directory`* .

Examples

The following example adds a security policy task entry to the policy named “policy1” on Vserver vs1.

```
cluster1::> vserver security file-directory policy task add -vserver vs1
-policy-name policy1 -path / -access-control slag -security-type ntfs
-ntfs-mode propagate -ntfs-sd sd -index-num 1
cluster1::> vserver security file-directory policy task add -vserver vs1
-policy-name policy2 -path /1 -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd1,sd2
              cluster1::> vserver security file-directory policy task show
Vserver: vs1
                Policy: policy1
Index  File/Folder  Access           Security  NTFS       NTFS Security
                         Path         Control          Type      Mode
Descriptor Name
                   -----  -----------  ---------------  --------
---------- ---------------
                   1      /            slag             ntfs
propagate  sd
Vserver: vs1
                Policy: policy2
Index  File/Folder  Access           Security  NTFS       NTFS Security
                         Path         Control          Type      Mode
Descriptor Name
                   -----  -----------  ---------------  --------
---------- ---------------
                   1      /1           file-directory   ntfs
propagate  sd1, sd2
```

vserver security file-directory policy task modify

Modify 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 modify` command modifies a task entry in a security policy.

> Modifying a policy task fails if a job is currently running for the specified policy in which a task is being modified.

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

> The only security type supported in this Data ONTAP release is *"ntfs"*; therefore, you cannot modify the `-security-type` parameter.

Parameters

`-vserver <vserver name>` - 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.

`[-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.

> 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.

`[-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* .

> 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 list of security descriptor names to apply to the path specified in the `-path` parameter.

Examples

The following example modifies the ntfs mode, index, and ntfs-sd parameters in the security policy task entry.

```
cluster1::> 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
cluster1::> vserver security file-directory policy task modify -vserver
vs1 -policy-name policy1 -path /1 -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd1, sd2 -index-num 2
cluster1::> vserver security file-directory policy task show -vserver vs1
-policy-name policy1
Vserver: vs1
                Policy: policy1
                 Index    File/Folder  Access          Security   NTFS
NTFS Security
                          Path         Control         Type       Mode
Descriptor Name
                 -----    --------     --------------  ------     -----
-----------------
                 1        /            file-directory  ntfs
propagate  sd
                 2        /1           file-directory  ntfs
propagate  sd1, sd2
```

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.

> Removing a policy task fails if a job is currently running for the specified policy from which a task is being removed.

Parameters

-vserver <vserver name> - 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.

```
cluster1::> 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

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 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.

[-index-num <integer>] - Position

If you specify this parameter, the command displays information only about tasks assigned the index number that you specify.

[-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.

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.

[-access-control {file-directory|slag}] - Access Control Level

If you specify this parameter, the command displays information only about tasks associated to the access control.

Examples

The following example displays policy task entries for a policy named “policy1” on Vserver vs1.

```
cluster1::> vserver security file-directory policy task show -vserver vs1
-policy-name policy1
Vserver: vs1
                  Policy: policy1
Index  File/Folder  Access           Security  NTFS       NTFS Security
                        Path         Control          Type      Mode
Descriptor Name
                  -----  -----------  ---------------  --------
---------- ---------------
                  1      /1           file-directory   ntfs      propagate
sd1, sd2
                  2      /2           file-directory   ntfs      ignore
-
2 entries were displayed.
```

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. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the permission trace is applied.

`-index <integer>` - Filter Index

This parameter 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.

`[-protocols {cifs|nfs}]` - Protocols

This parameter specifies the protocols for which the permission trace is created. If the `-protocols` parameter is not specified, the filter will only apply to the CIFS protocol.

`[-client-ip <IP Address>]` - Client IP Address to Match

This parameter specifies the IP Address from which the user is accessing the Vserver.

`[-path <TextNoCase>]` - Path

This parameter specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share (for a CIFS filter) or the root of the junction path (for an NFS filter) 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 parameter 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 or User ID `}`

This parameter specifies the UNIX user name to trace. It accepts UNIX user ID only for NFS filters.

`[-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 parameter specifies whether to enable or disable the filter. Filters are enabled by default.

[-time-enabled <integer>] - Minutes Filter is Enabled

This parameter specifies a timeout for this filter, after which it is deleted.

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, these filters are deleted when the time specified in the time enabled field elapses.The default value for the time-enabled option is 60 min. If the client is accessing a file with the path \\server\sharename\dir1\dir2\dir3\file.txt, for a filter applicable to CIFS, 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
```

Similarly, while creating a filter for NFS, if -path option is specified and the client is accessing a file with path /junction_path1/junction_path2/dir1/file.txt, a complete path starting from the last junction path or a partial path can be given as shown:

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols nfs -path dir1/file.txt
```

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols nfs -path file.txt
```

The following example creates a filter that is applicable to both CIFS and NFS.

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols cifs,nfs -unix-user root
```

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. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the tracing filter entry that you want to delete is applied.

`-index <integer>` - Filter Index

This parameter 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
```

Related Links

- 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. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the permission trace is applied.

-index <integer> - Filter Index

This parameter 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.

[-protocols {cifs|nfs}] - Protocols

This parameter specifies the protocols for which the permission trace is created.

[-client-ip <IP Address>] - Client IP Address to Match

This parameter specifies the IP Address from which the user is accessing the Vserver.

[-path <TextNoCase>] - Path

This parameter specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share (for a CIFS filter) or the root of the junction path (for an NFS filter) 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 parameter 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 or User ID }

This parameter specifies the UNIX user name to trace. It accepts UNIX user ID only for NFS filters.

[-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 parameter specifies whether to enable or disable the filter. Filters are enabled by default.

[-time-enabled <integer>] - Minutes Filter is Enabled

This parameter specifies a timeout for this filter, after which it is deleted.

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, for a filter applicable to CIFS, 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
```

Similarly, for filters applicable to NFS, if -path option is specified and the client is accessing a file with path /junction_path1/junction_path2/dir1/file.txt, a complete path starting from the last junction path or a partial path can be given as shown:

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols nfs -path dir1/file.txt
```

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols nfs -path file.txt
```

The following example modifies a filter that is applicable to both CIFS and NFS.

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols cifs,nfs -unix-user root -path 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. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the 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

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.

[-protocols {cifs|nfs}] - Protocols

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified protocols.

[-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 or User ID

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified UNIX user name or user ID(for NFS specififc filters).

[-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 about the time durations configured for filters during creation.

Examples

The following example displays security trace filters for Vserver *vserver1* .

```
cluster1::> vserver security trace filter show
Vserver  Index   Client-IP     Path          Trace-Allow Windows-Name
Protocol
-------- ----- ------------ ---------------- ----------- -------------
--------
vserver1 1     -            -               no          domain\user
cifs
vserver1 2     192.168.2.3  -               yes         -
cifs
vserver1 3     -            /dir1/dir2/file  no          domain\
cifs
                                                        administrator
vserver1 4     -            file            yes         -             nfs
4 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.
```

Parameters

-node {<nodename>|local} - Node

This parameter specifies the cluster node on which the permission tracing event that you want to delete occurred.

-vserver <vserver name> - Vserver

This parameter specifies the Vserver on which the permission tracing event that you want to delete occurred.

-seqnum <integer> - Sequence Number

This parameter 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_`` .
```

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 name>] - 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.

[-win-user <TextNoCase>] - Windows User Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified Windows 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 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, the location where access is either allowed or denied, and the access right for which the file operation is 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
* Access is allowed because storage-level access guard (SLAG) grants requested access
* Access is allowed because no central access policies applied
* Access is allowed because no central access policies could be applied from the corrupt SACL
* Access is allowed because matching central access policy could not be located
* Access is allowed because no central access rules apply to the object
* Access is allowed because skipped one or more corrupt central access rules
* Access is allowed because all evaluated central access rules grant 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
- Access is denied as the volume is readonly or directory is a snapshot
- Access is denied. System attribute is not set in the request
- Access is denied by the storage-level access guard (SLAG)
- Access is denied, file is infected
- Access is denied. Central access policy DB not ready
- Access is denied. Central access rule is corrupt
- Access is denied. Central access rule explicitly denied access
- Access is denied. Matching central access policy not found
- Access is denied because the user does not have UNIX root privileges
- Access is denied because the UNIX user could not be mapped to a valid NT user
- Access is denied because the UNIX permissions/uid/gid/NFSv4 ACL cannot be set in an NTFS qtree

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.
- while truncating a file.
- while truncating a system file.
- while appending to a file or setting a file attribute.
- while opening a file or directory for delete.
- while checking for permission on parent directory during create.
- while appending to the file.
- while creating the device file.
- while reading the user’s access rights on an object.

The access rights for which the file operation is allowed or denied are as follows:

+

- Append.
- Delete.
- Delete Child.
- Execute.
- Generic All.
- Generic Execute.
- Generic Read.
- Generic Write.
- Maximum Allowed.
- Read.
- Read Attributes.
- Read Control.
- Read EA.
- System Security.
- Synchronize.
- Write.
- Write Attributes.

- Write DAC.
- Write EA.
- Write Owner.
- None.

[-unix-user <TextNoCase>] - 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 access by the specified UNIX user.

[-session-id <integer>] - CIFS Session ID

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified CIFS session ID.

[-share-name <TextNoCase>] - Accessed CIFS Share Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified CIFS share name.

[-protocol {cifs|nfs}] - Protocol

If you specify this parameter, the command displays information only about the security trace events that occurred for the specified protocol.

[-volume-name <TextNoCase>] - Accessed Volume Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified volume name.

Examples

The following example displays information about security trace records:

```
cluster1::> vserver security trace trace-result show
Vserver: vserver_1

Node                     Index     Filter Details      Reason
------------------------ -------- ---------------------
-------------------------
cluster1-01              1         Security Style: MIXED Access is allowed
because
                                   and NT ACL            CIFS implicit
permission
                                                         grants requested
access
                                                         while opening
existing
                                                         file or directory.
                                                         Access is granted
for:
                                                         "Read Attributes"
                                   Protocol: cifs
                                   Share: sh1
                                   Path: /stk/bit
                                   Win-User: cifs1\
                                   administrator
                                   Unix-User: root
                                   Session-ID: 58455810

1 entries were displayed.
```

The following example displays information about security trace records for path /stk/bit/set:

```
cluster1::> vserver security trace trace-result show -path /stk/bit/set

Vserver: vserver_1

Node                     Index     Filter Details      Reason
------------------------ -------- ---------------------
-------------------------
cluster1-01              1         Security Style: MIXED Access is allowed
because
                                   and UNIX permissions  the user has UNIX
root
                                                         privileges while
opening
                                                         existing file or
                                                         directory.
```

```
                                                    Access is granted
for: "Read"
                                Protocol: cifs
                                Share: sh1
                                Path: /stk/bit/set
                                Win-User: cifs1\
                                administrator
                                UNIX-User: root
                                Session-ID: 75435293758455810
cluster1-01             1       Security Style: MIXED Access is denied.
The
                                and NT ACL            requested
permissions
                                                      are not granted by
the
                                                      ACE while checking
for
                                                      child-delete access
on
                                                      the parent. Access
is not
                                                      granted for:
"Delete Child"
                                Protocol: cifs
                                Share: sh1
                                Path: /stk/bit/set
                                Win-User: cifs1\
                                administrator
                                UNIX-User: root
                                Session-ID: 75435293758455324
cluster1-01             1       Security Style: MIXED Access is allowed
because
                                and NT ACL            the CIFS user is
owner.
                                                      Access is denied by
an
                                                      explicit ACE while
                                                      setting the
attributes.
                                                      Access is not
granted for:
                                                      "Read Attributes"
Protocol: cifs
                                Share: sh1
                                Path: /stk/bit/set
                                Win-User: cifs1\
```

```
                                  administrator
                                  UNIX-User: root
                                  Session-ID: 75435293758455324
3 entries were displayed.
```

The following example displays information about security trace records for the protocol nfs:

```
cluster1::> vserver security trace trace-result show -protocol nfs
Vserver: vserver_1

Node            Index Filter Details             Reason
--------------- ----- -------------------------
------------------------------
cluster1-01     2     Security Style: UNIX       Access is allowed because
the
                      permissions                user has UNIX root
privileges
                                                 while setting attributes.
                      Protocol: nfs
                      Volume: testvol_flex
                      Share: -
                      Path: /f1
                      Win-User: -
                      UNIX-User: root
                      Session-ID: -
cluster1-01     2     Security Style: UNIX       Access is allowed because
the
                      permissions                user has UNIX root
privileges
                                                 while writing to the
file.
                                                 Access is granted for:
"Write"
                      Protocol: nfs
                      Volume: testvol_flex
                      Share: -
                      Path: /f1
                      Win-User: -
                      UNIX-User: root
                      Session-ID: -
cluster1-01     3     Security Style: UNIX       Access is denied by UNIX
                      permissions                permissions while
creating
                                                 the file. Access is not
                                                 granted for:
```

```
"Synchronize",
                                                    "Read Control", "Read
                                                    Attributes", "Execute",
                                                    "Write"
                      Protocol: nfs
                      Volume: testvol_flex
                      Share: -
                      Path: /d1/file
                      Win-User: -
                      UNIX-User: 1029
                      Session-ID: -
3 entries were displayed.
```

Related Links

- vserver security trace filter create

vserver services commands

vserver services access-check authentication get-claim-name

Get the Name of a Claim

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

Description

The `vserver services access-check authentication get-claim-name` command obtains the display name for a given claim.

Parameters

`[-node {<nodename>|local}]` - Node Name (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

`-claim-cn <text>` - Claim CN (privilege: advanced)

The claim ID of the claim display name.

Examples

This example gets the display name of a claim for the CIFS server created on Vserver vs2

```
cluster1::vserver services access-check*> authentication get-dc-info -node
vsim1 -vserver vs2 -claim-cn ad://ext/accountExpires:88d065c21536d9fe

Name of claim ad://ext/accountExpires:88d065c21536d9fe: accountExpires
```

vserver services access-check authentication get-dc-info

Get Domain Controller Information

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

Description

The `vserver services access-check authentication get-dc-info` command obtains information about one of the Domain Controllers (DC) for the domain of which the CIFS server is a member. The information fetched is the Forest and Domain of which the DC is a member, the NetBIOS name of the Domain, the NetBIOS Hostname of the DC, the CIFS Server site, the CIFS Client site, GUID of the domain and flags. Flags describe the features and roles of the DC.

Parameters

`[-node {<nodename>|local}]` - Node Name (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

Examples

This example gets the information about a Domain Controller for CIFS server created on Vserver vs2.

```
cluster1::vserver services access-check*> authentication get-dc-info -node
vsim2-d1-01 -vserver vs2
DC Information:
 ---------------
          Forest: cifs.lab.netapp.com
          Domain: cifs.lab.netapp.com
    NetBIOS Name: CIFSLAB
NetBIOS Hostname: A7-6
     Server Site: cifs-dev-j4
     Client Site:
            GUID: 0366BE1F-FA08-4747-B5AC56097189C90E
           Flags: 0x00000178
                  DS_LDAP_FLAG
                  DS_DS_FLAG
                  DS_KDC_FLAG
                  DS_TIMESERV_FLAG
                  DS_WRITABLE_FLAG
                  DS_PING_FLAGS
```

vserver services access-check authentication login-cifs

Authenticate a CIFS user

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

Description

The `vserver services access-check authentication login-cifs` command authenticates a Windows user through the specified node using the specified Vserver's configuration. Upon success, it displays the user's Windows and UNIX credentials.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of a Vserver with a configured CIFS server.

`-user <text>` - Windows Name (privilege: advanced)

The name of a user that is a member of the Windows or a trusted domain that the CIFS server in the specified Vserver belongs to.

`[-clientIp <IP Address>]` - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

Examples

This example authenticates the Windows user "administrator" through node "node2" using the configuration of "vs1." Upon success, it displays the Windows and UNIX credentials for user "administrator."

```
cluster1::vserver services access-check*> authentication login-cifs
-vserver vs1 -user administrator -node node2

Enter the password:
Windows User: administrator Domain: EXAMPLE Privs: a7
 Primary Grp: S-1-5-21-1407423728-2963865486-1834115207-513
      Domain: S-1-5-21-1407423728-2963865486-1834115207 Rids: 500, 520,
513, 22226, 26625, 1842, 512, 519, 518, 8323, 1645, 1648, 1644, 1647
      Domain: S-1-1 Rids: 0
      Domain: S-1-5 Rids: 11, 2
     Unix ID: 0, GID: 0
       Flags: 1
   Domain ID: 0
  Other GIDs:
Authentication Succeeded.
```

vserver services access-check authentication ontap-admin-login-cifs

Authenticate Data ONTAP admin CIFS user

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

Description

The `vserver services access-check authentication ontap-admin-login-cifs` command authenticates the Data ONTAP administrator's user through the specified node using the specified Vserver's configuration. Upon success, it displays the user's Windows credentials.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of a Vserver with a configured CIFS server.

`-user <text>` - User Name (privilege: advanced)

The name of a user that is a member of the Windows or a trusted domain that the CIFS server in the specified Vserver belongs to.

`[-clientIp <IP Address>]` - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

Examples

This example authenticates the Data ONTAP administrator user "administrator" through node "node2" using the configuration of Vserver "vs1." Upon success, it displays the CIFS credentials for "administrator."

```
cluster1::vserver services access-check*> authentication ontap-admin-
login-cifs -vserver vs1 -user administrator -node node2

Enter the password:
Windows User: administrator Domain: EXAMPLE Privs: a7
 Primary Grp: S-1-5-21-1407423728-2963865486-1834115207-513
      Domain: S-1-5-21-1407423728-2963865486-1834115207 Rids: 500, 520,
513, 22226, 26625, 1842, 512, 519, 518, 8323, 1645, 1648, 1644, 1647, 1003
      Domain: S-1-1 Rids: 0
      Domain: S-1-5 Rids: 11, 2
Authentication Succeeded.
```

vserver services access-check authentication show-creds

Display a user's credentials based on a UNIX UID or Windows SID

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

Description

The `vserver services access-check authentication show-creds` command returns the credentials for a Windows user using SID, a Windows user using a Windows username, a UNIX user using UID, or a UNIX user using a UNIX user name. This command is useful for retrieving information such as account type, SIDs, UIDs, GIDs, privileges, and domain or group membership.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The command displays information for the specified Vserver.

{ `-uid <integer>` - UID (privilege: advanced)

The UNIX user's UID.

| `-sid <text>` - SID (privilege: advanced)

The Windows user's SID.

| `-unix-user-name <text>` - Unix User Name (privilege: advanced)

The UNIX username.

| -win-name <text> - Windows Name (privilege: advanced) }

The Windows username.

[-list-name {true|false}] - Display Translated Names (privilege: advanced)

If this parameter is specified, the command displays information as translated names.

[-list-id {true|false}] - Display IDs (privilege: advanced)

If this parameter is specified, the command displays information as IDs.

[-clientIp <IP Address>] - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

[-skip-domain-group {true|false}] - Skip Domain Groups (privilege: advanced)

If this parameter is specified, Windows domain group membership will not be fetched and only local group membership will be displayed, if any.

Examples

This example returns credential information for UNIX user with UID "0" on node "node1" for Vserver "vs1."

```
cluster1::*> vserver services access-check authentication show-creds -node
node1 -vserver vs1 -uid 0
(vserver services access-check authentication show-creds)
UNIX UID: root <> Windows User: CIFSQA\Administrator (User)
GID: root
 Supplementary GIDs: <None>
Windows Membership:
  CIFSQA\Schema Admins (Domain group)
  CIFSQA\Enterprise Admins (Domain group)
  CIFSQA\Domain Admins (Domain group)
  CIFSQA\Domain Users (Domain group)
  CIFSQA\Group Policy Creator Owners (Domain group)
  BUILTIN\Administrators (Alias)
  BUILTIN\Users (Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users
Privileges (0x2b7):
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
```

This example returns credential information for UNIX user with UID "0" on node "node1" for Vserver "vs1" when list-name "false" and list-id "true."

```
cluster1::*> vserver services access-check authentication show-creds -node
node1 -vserver vs1 -uid 0 -list-name false -list-id true
(vserver services access-check authentication show-creds)
UNIX UID: 0 <> Windows User: S-1-5-21-1407423728-2963865486-1834115207-500
GID: 0
 Supplementary GIDs: <None>
Windows Membership:
  S-1-5-21-1407423728-2963865486-1834115207-518
  S-1-5-21-1407423728-2963865486-1834115207-519
  S-1-5-21-1407423728-2963865486-1834115207-512
  S-1-5-21-1407423728-2963865486-1834115207-513
  S-1-5-21-1407423728-2963865486-1834115207-520
  S-1-5-32-544
  S-1-5-32-545
 User is also a member of S-1-1-0, S-1-5-11, and S-1-5-2
Privileges (0x2b7):
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
```

This example returns credential information for UNIX user with UID "0" on node "node1" for Vserver "vs1" when list-name "true" and list-id "true."

```
cluster1::*> vserver services access-check authentication show-creds -node
node1 -vserver vs1 -uid 0 -list-name false -list-id true
(vserver services access-check authentication show-creds)
UNIX UID: 0 (root) <> Windows User: S-1-5-21-1407423728-2963865486-
1834115207-500 (CIFSQA\Administrator (User))
GID: 0 (root)
 Supplementary GIDs: <None>
Windows Membership:
  S-1-5-21-1407423728-2963865486-1834115207-518     CIFSQA\Schema Admins
(Domain group)
  S-1-5-21-1407423728-2963865486-1834115207-519     CIFSQA\Enterprise
Admins (Domain group)
  S-1-5-21-1407423728-2963865486-1834115207-512     CIFSQA\Domain Admins
(Domain group)
  S-1-5-21-1407423728-2963865486-1834115207-513     CIFSQA\Domain Users
(Domain group)
  S-1-5-21-1407423728-2963865486-1834115207-520     CIFSQA\Group Policy
Creator Owners (Domain group)
  S-1-5-32-544      BUILTIN\Administrators (Alias)
  S-1-5-32-545      BUILTIN\Users (Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users
Privileges (0x2b7):
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
```

This example returns credential information for UNIX user with UID "0" on node "node1" for Vserver "vs1" when list-name "true" and list-id "false."

```
cluster1::*> vserver services access-check authentication show-creds -node
node1 -vserver vs1 -uid 0 -list-name true -list-id false
(vserver services access-check authentication show-creds)
UNIX UID: root <> Windows User: CIFSQA\Administrator (User)
GID: root
 Supplementary GIDs: <None>
Windows Membership:
  CIFSQA\Schema Admins (Domain group)
  CIFSQA\Enterprise Admins (Domain group)
  CIFSQA\Domain Admins (Domain group)
  CIFSQA\Domain Users (Domain group)
  CIFSQA\Group Policy Creator Owners (Domain group)
  BUILTIN\Administrators (Alias)
  BUILTIN\Users (Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users
Privileges (0x2b7):
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
```

vserver services access-check authentication show-ontap-admin-unix-creds

Display Data ONTAP admin Unix credentials based on username or user ID

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

Description

The `vserver services access-check authentication show-ontap-admin-unix-creds` uses the Vserver's ns-switch configuration to determine and display Data ONTAP administrator's UNIX information.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)
The name of the node on which the command is executed.

`-vserver <vserver>` - Vserver (privilege: advanced)
The name of the Vserver.

{ `-unix-user-name <text>` - Unix User Name (privilege: advanced)
The UNIX username.

| `-uid <integer>` - Unix User ID (privilege: advanced) }
The UID of a UNIX user.

Examples

This example shows Data ONTAP administrator's UNIX user's UID, GID, home directory, and login shell for user "root" on Vserver "vs1" for node "node2."

```
cluster1::vserver services access-check*> authentication show-ontap-admin-
unix-creds -vserver vs1 -unix-user-name root -node node2
       User ID: 0
      Group ID: 1
Home Directory: /
   Login Shell: /bin/csh
```

vserver services access-check authentication sid-to-uid

Translate a Windows SID to a UNIX user ID

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

Description

The `vserver services access-check authentication sid-to-uid` translates a Windows SID to a UNIX UID.

Parameters

`[-node {<nodename>|local}]` - Node Name (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

`-sid <text>` - Windows SID (privilege: advanced)

The SID of a Windows user.

`[-clientIp <IP Address>]` - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

Examples

This example translates a Windows SID on node "node2" and returns the corresponding UNIX user's UID.

```
cluster1::vserver services access-check*> sid-to-uid -vserver vs1 -sid S-
1-5-21-1407423728-2963865486-1834115207-500 -node node2
UID: 0
```

vserver services access-check authentication sid-to-unix-name

Translate a Windows SID to a UNIX User Name

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

Description

The `vserver services access-check authentication sid-to-unix-name` translates a Windows SID to a UNIX Name.

Parameters

`[-node {<nodename>|local}]` - Node Name (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

`-sid <text>` - Windows SID (privilege: advanced)

The Windows SID which is to be translated to the corresponding UNIX name.

Examples

This example translates a Windows SID on node "node2" and returns the corresponding UNIX name.

```
cluster1::vserver services access-check*> sid-to-unix-name -node node2
-vserver vs1 -sid S-1-5-21-1407423728-2963865486-1834115207-500
    SID Type: User
   UNIX Name: test
 Domain Name: TESTDOMAIN
Windows Name: test
```

vserver services access-check authentication translate

Translate between Various Names and Their Identifiers

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

Description

The `vserver services access-check authentication translate` command translates SIDs, UIDs, and GIDs to names. If you enter a SID, the command returns a Windows name; if you enter a Windows name, the command returns a SID; if you enter a UNIX username, the command returns a UID; if you enter a UID, the command returns a UNIX username; if you enter a GID, the command returns a UNIX group name; if you enter a UNIX group-name, the command returns a GID.

Parameters

[-node {<nodename>|local}] - Node Name (privilege: advanced)
The name of the node on which the command is executed.

-vserver <vserver> - Vserver Name (privilege: advanced)
The name of the Vserver.

{ -uid <integer> - UNIX User ID (privilege: advanced)
The UNIX user's UID.

| -gid <integer> - UNIX Group ID (privilege: advanced)
The UNIX user's GID.

| -sid <text> - Windows SID (privilege: advanced)
The Windows user's SID.

| -unix-user-name <text> - UNIX User Name (privilege: advanced)
The UNIX username.

| -unix-group-name <text> - UNIX Group Name (privilege: advanced)
The UNIX group name.

| -win-name <text> - Windows Name (privilege: advanced) }
The Windows name.

Examples

This example translates the UNIX UID 0 to username "root" on node "node2" for Vserver "vs1."

```
cluster1::vserver services access-check*> authentication translate
-vserver vs1 -uid 0 -node node2
root
```

This example translates and the Windows username "administrator" to the corresponding SID on node "node2" for Vserver "vs1."

```
cluster1::vserver services access-check*> authentication translate
-vserver vs1 -win-name administrator -node node2
S-1-5-21-1407423728-2963865486-1834115207-500
```

vserver services access-check authentication uid-to-sid

Translate a UNIX user ID to a Windows SID

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

Description

The `vserver services access-check authentication uid-to-sid` translates a UNIX UID to a Windows SID.

Parameters

`[-node {<nodename>|local}]` - Node Name (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

`-uid <integer>` - UNIX User ID (privilege: advanced)

The user ID of a UNIX user.

`[-clientIp <IP Address>]` - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

Examples

This example translates a UNIX user's UID on node "node2" and returns the corresponding SID.

```
cluster1::vserver services access-check*> uid-to-sid -vserver vs1 -uid 0
-node node2
SID: S-1-5-21-1407423728-2963865486-1834115207-500
```

vserver services access-check dns forward-lookup

Perform DNS forward lookup

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

Description

The `vserver services access-check dns forward-lookup` returns the IP address of a hostname based on the lookup done on the DNS server specified or the Vserver's DNS configuration.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

This specifies the name of the node on which the command is executed.

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

This specifies the name of the Vserver.

`-hostname <text>` - Hostname (privilege: advanced)

This specifies the hostname to be looked up on the DNS server.

[-lookup-type {ipv4|ipv6|all}] - Lookup Type (default: all) (privilege: advanced)

This specifies the type of IP address to be looked up on the DNS server. If you specify "all", it looks up both IPv4 and IPv6 addresses.

Examples

The following example returns the IPv6 addresses of the hostname "example" in Vserver "vs1" from the node "node2".

```
cluster1::vserver services access-check*> dns forward-lookup -vserver vs1
-node node2
-domains example.com -name-servers 10.72.46.234 -hostname example -lookup
-type ipv6
6ffe::1
3ffe::1
```

vserver services access-check dns srv-lookup

Perform DNS lookup for SRV records

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

Description

The `vserver services access-check dns srv-lookup` returns the IP addresses of a host that is providing the specified service in the network, based on the SRV record lookup done on the Vserver's DNS server.

Parameters

[-node {<nodename>|local}] - Node (privilege: advanced)

This specifies the name of the node on which the command is executed.

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

This specifies the name of the Vserver.

[-name-servers <IP Address>,…] - Name Servers (privilege: advanced)

This specifies the DNS servers in which the hostname lookup needs to be done.

-lookup-string <text> - Name to Lookup For (privilege: advanced)

This specifies the complete string for which SRV record needs to be looked up on the DNS server.

[-lookup-type {ipv4|ipv6|all}] - Lookup Type (default: all) (privilege: advanced)

This specifies the type of IP address to be looked up on the DNS server. If you specify "all", it looks up both IPv4 and IPv6 addresses. The lookup string must be in the form "service.protocol.domain".

Examples

The following example returns the IPv6 addresses of the host providing "http" service on "tcp" protcocol in

Vserver "vs1" from the node "node2".

```
cluster1::vserver services access-check*> dns srv-lookup -vserver vs1
-node node2
-lookup-string _http._tcp.nw7.na -lookup-type ipv6
9ffe::1
5ffe::1
```

vserver services access-check name-mapping show

Display or verify name mapping configuration

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

Description

The `vserver services access-check name-mapping show` command tests the name mapping configuration for the specified Vserver on the specified node. The command can perform name mapping for Kerberos to UNIX, Windows to UNIX, and UNIX to Windows directions.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

`-direction {krb-unix|win-unix|unix-win}` - Mapping Direction (privilege: advanced)

The mapping direction.

`-name <text>` - Name (privilege: advanced)

The username.

`[-clientIp <IP Address>]` - Client IP Address (privilege: advanced)

The IP address of the client as specified by the user

Examples

This example shows a name mapping on Vserver "vs1" from UNIX username "root," which is mapped to a Windows name "EXAMPLE\Administrator" on node "node2."

```
cluster1::vserver services access-check*> name-mapping show -vserver vs1
-direction unix-win -name root -node node2
root maps to EXAMPLE\Administrator
```

This example shows a name mapping on Vserver "vs1" from Windows name "EXAMPLE\Administrator" to a UNIX name "root."

```
cluster1::vserver services access-check*> name-mapping show -vserver vs1
-direction win-unix -name EXAMPLE\Administrator -node node2
EXAMPLE\Administrator maps to root
```

vserver services access-check server-discovery reset

Reset server discovery information for a Vserver

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

Description

The `vserver services access-check server-discovery reset` command deletes all of the discovered server information for a given Vserver on the given node. It returns a success message upon deleting. The next attempt to access external servers will trigger the server discovery process to acquire up-to-date server information.

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver on which you want to delete all of the discovered server information.

Examples

This example deletes all of the discovered server information for Vserver "vs1" on the node "node2."

```
cluster1::vserver services access-check*> server-discovery reset -vserver
vs1 -node node2
Discovery Reset succeeded for Vserver: vs1
```

vserver services access-check server-discovery show-host

Display information about service host machines

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

Description

The `vserver services access-check server-discovery show-host` command displays information about service host machines.

Parameters

[-node {<nodename>|local}] - Node (privilege: advanced)

The name of the node on which the command is executed.

Examples

This example shows the host name and IP Address for five different service host machines.

```
cluster1::vserver services access-check*> server-discovery show-host
  Host Name: 172.19.3.11
Cifs Domain:
  AD Domain:
 IP Address: 172.19.3.11
Host Name: example-dc-1
Cifs Domain:
  AD Domain:
 IP Address: 172.17.152.40
Host Name: example-dc-2
Cifs Domain:
  AD Domain:
 IP Address: 172.17.152.41
Host Name: example-dc-3
Cifs Domain:
  AD Domain:
 IP Address: 172.17.152.42
Host Name: example-dc-4
Cifs Domain:
  AD Domain:
 IP Address: 172.17.152.43
```

vserver services access-check server-discovery show-site

Display site membership

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

Description

The `vserver services access-check server-discovery show-site` command displays the site membership for a given Vserver on a given node.

Parameters

[-node {<nodename>|local}] - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver.

Examples

This example shows the site membership for Vserver "vs1" from the perspective of node "node2".

```
cluster1::vserver services access-check*> server-discovery show-site -node
node2 -vserver vs1
california
```

vserver services access-check server-discovery test

Verify server discovery

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

Description

The command `vserver services access-check server-discovery test` completes the entire discovery including domain controller (DC), LDAP, and NIS servers for the default domain for a given Vserver on a given node. The Vserver must have CIFS configured for it to run successfully. If the discovery is successful, the command returns a success message. The discovered server information can be seen using the command `vserver cifs domain discovered-servers` .

Parameters

`[-node {<nodename>|local}]` - Node (privilege: advanced)

The name of the node on which the command is executed.

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

The name of the Vserver on which you want to test all of the discovered server information.

Examples

This example tests all of the discovered server information on Vserver "vs1" on node "node2."

```
cluster1::vserver services access-check*> server-discovery test -vserver
vs1 -node node2
Discovery Global succeeded for Vserver: vs1
```

vserver services name-service cache group-membership delete-all

Delete all the entries for the vserver

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

Description

The vserver services name-service cache group-membership delete command removes the cached group membership entries of the users for the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the group membership entries need to be deleted.

Examples

The following example deletes all the cached group membership entries for Vserver vs0:

```
cluster1::> vserver services name-service cache group-membership delete-
all -vserver vs0
```

Related Links

- vserver services name-service cache group-membership delete

vserver services name-service cache group-membership delete

Delete an entry

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

Description

The `vserver services name-service cache group-membership delete` command removes the cached group membership entries of the users.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the group membership entries need to be deleted.

`-user <text>` - User Name (privilege: advanced)

Use this parameter to specify the user name for which the cached group membership entries need to be deleted.

`-group <integer>` - Gid (privilege: advanced)

Use this parameter to specify the primary group identifier or GID for which the cached group membership entries need to be deleted.

Examples

The following example deletes all the cached group membership entries for Vserver vs0, user 'a' and group '1':

```
cluster1::> vserver services name-service cache group-membership delete
-vserver vs0 -user a -group 1
```

vserver services name-service cache group-membership show

Display group list

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

Description

The `vserver services name-service cache group-membership show` command displays the cached group membership information of the 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] }

Use this parameter to display detailed information about the cached group membership details of the user.

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

Use this parameter to specify the Vserver for which the group membership entries need to be displayed.

[-user <text>] - User Name (privilege: advanced)

Use this parameter to display information only about the cached group membership entries that have the specified user name.

[-group <integer>] - Gid (privilege: advanced)

Use this parameter to display information only about the cached group membership entries of the users that have the specified primary group identifier or GID.

[-ngroups <integer>] - Number of Groups (privilege: advanced)

Use this parameter to display information only about the cached group membership entries of the users who belong to the specified number of groups.

[-groups <integer>,…] - Group List (privilege: advanced)

Use this parameter to display information only about the cached group membership entries of the users who belong to the specified group identifiers or GIDs.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the group membership entries that were cached at the specified time.

[-is-partial {true|false}] - Is Partial Result (privilege: advanced)

Use this parameter to display information only about the group membership entries that have the specified value for partial result. The Value *`true`* displays only the cached entries that have partial result and the value *`false`* displays only the cached entries that do not have partial result.

Examples

The following example displays the group membership details of the users for all the vservers:

```
cluster1::> vserver services name-service cache group-membership show
```

The following example displays all the group membership details of the users for Vserver vs0:

```
cluster1::> vserver services name-service cache group-membership show
-vserver vs0
```

vserver services name-service cache group-membership settings modify

Modify Group Membership Cache Configuration

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

Description

The `vserver services name-service cache group-membership settings modify` command modifies the group membership cache configuration of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the group membership cache settings need to be modified.

`[-is-enabled {true|false}]` - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the group membership database. The value *`true`* means the cache is enabled and the value *`false`* means the cache is diabled. The default value for this parameter is *`true`* .

`[-grplist-ttl <[<integer>h][<integer>m][<integer>s]>]` - Time to Live for Grplist (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the group membership entries need to be cached. The default value is 1 hour.

Examples

The following example modifies the group membership cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache group-membership settings
modify -vserver vs0 -grplist-ttl 600
```

The following example disables the group membership cache for Vserver vs0:

```
cluster1::> vserver services name-service cache group-membership settings
modify -vserver vs0 -is-enabled false
```

vserver services name-service cache group-membership settings show

Display Group Membership Cache Configuration

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

Description

The `vserver services name-service cache group-membership settings show` command displays information about the group membership cache configuration for the 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] }

Use this parameter to display detailed information about the group membership cache configuration settings.

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

Use this parameter to display information about the group membership cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the group membership cache configuration settings that have the specified cache enabled setting. The value *`true`* displays only the entries that have cache enabled and the value *`false`* displays only the entries that have cache disabled.

[-grplist-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live for Grplist (privilege: advanced)

Use this parameter to display information only about the group membership cache configuration settings that have the specified Time to Live.

Examples

The following example shows the group membership cache configuration settings for all the Vservers:

```
cluster1::> vserver services name-service cache group-membership settings
show
```

The following example shows the group membership cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache group-membership settings
show -vserver vs0
```

vserver services name-service cache hosts forward-lookup delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache hosts forward-lookup delete-all` command removes all the cached host to IP lookup entries for a Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached forward lookup entries need to be deleted.

Examples

The following example deletes all the cached forward lookup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts forward-lookup
delete-all -vserver vs0
```

vserver services name-service cache hosts forward-lookup delete

Delete an entry

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

Description

The `vserver services name-service cache hosts forward-lookup delete` command removes a cached host to IP lookup entry.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached forward lookup table entries need to be deleted.

`-host <text>` - Hostname (privilege: advanced)

Use this parameter to specify the hostname of the cached forward lookup table entries that need to be deleted.

-protocol {Any|ICMP|TCP|UDP} - Protocol (privilege: advanced)

Use this parameter to specify the protocol of the cached forward lookup table entries that need to be deleted.

-sock-type {SOCK_ANY|SOCK_STREAM|SOCK_DGRAM|SOCK_RAW} - Sock Type (privilege: advanced)

Use this parameter to specify the socket type of the cached forward lookup table entries that need to be deleted.

-flags {FLAG_NONE|AI_PASSIVE|AI_CANONNAME|AI_NUMERICHOST|AI_NUMERICSERV} - Flags (privilege: advanced)

Use this parameter to specify the flag of the cached forward lookup table entries that need to be deleted.

-family {Any|Ipv4|Ipv6} - Family (privilege: advanced)

Use this parameter to specify the family of the cached forward lookup table entries that need to be deleted.

Examples

The following example deletes the cached forward lookup entry for Vserver vs0 and host "abc":

```
cluster1::> vserver services name-service cache hosts forward-lookup
delete -vserver vs0 -host abc
```

vserver services name-service cache hosts forward-lookup show

Display host-byname struct

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

Description

The `vserver services name-service cache hosts forward-lookup show` command displays the cached host to IP lookup entries.

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] }

Use this parameter to display detailed information about the cached forward lookup table entries.

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

Use this parameter to specify the Vserver for which the cached forward lookup table entries need to be displayed.

[-host <text>] - Hostname (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified hostname.

[-protocol {Any|ICMP|TCP|UDP}] - Protocol (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specifed protocol.

[-sock-type {SOCK_ANY|SOCK_STREAM|SOCK_DGRAM|SOCK_RAW}] - Sock Type (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified socket type.

[-flags {FLAG_NONE|AI_PASSIVE|AI_CANONNAME|AI_NUMERICHOST|AI_NUMERICSERV}] - Flags (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified flags.

[-family {Any|Ipv4|Ipv6}] - Family (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified family.

[-canonname <text>] - Canonical Name (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified canonical name.

[-ips <IP Address>,…] - IP Addresses (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified IPs.

[-ip-protocol {Any|ICMP|TCP|UDP}] - Protocol (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified protocol of the resolved IP address from forward lookup.

[-ip-sock-type {SOCK_ANY|SOCK_STREAM|SOCK_DGRAM|SOCK_RAW}] - Sock Type (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified socket type of the resolved IP address from forward lookup.

[-ip-family {Any|Ipv4|Ipv6}] - Family (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified IP address family of the resolved IP address from forward lookup.

[-ip-addr-length <integer>,…] - Length (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified IP address length of the resolved IP address from forward lookup.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified IP source of the resolved IP address from forward lookup.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified time when the entry was cached.

[-ttl <integer>] - DNS TTL (privilege: advanced)

Use this parameter to display information only about the cached forward lookup table entries that have the specified Time To Live.

Examples

The following example displays all the cached forward lookup entries:

```
cluster1::> vserver services name-service cache hosts forward-lookup show
```

The following example displays all the cached forward lookup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts forward-lookup show
-vserver vs0
```

vserver services name-service cache hosts reverse-lookup delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache hosts reverse-lookup delete-all` command removes all the cached IP to host lookup entries for a Vserver.

Parameters

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

Use this parameter to specify the Vserver whose cached reverse lookup entries need to be deleted.

Examples

The following example deletes all the cached reverse lookup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts reverse-lookup
delete-all -vserver vs0
```

vserver services name-service cache hosts reverse-lookup delete

Delete an entry

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

Description

The `vserver services name-service cache hosts reverse-lookup delete` command removes a cached IP to host lookup entry.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached reverse lookup table entries need to be deleted.

`-ip <IP Address>` - IP Address (privilege: advanced)

Use this parameter to specify the IP address of the cached reverse lookup table entries that need to be deleted.

`-serv-flag <integer>` - Service flags (privilege: advanced)

Use this parameter to specify the service flag of the cached reverse lookup table entries that need to be deleted.

Examples

The following example deletes the cached reverse lookup entry for Vserver vs0 and IP address 1.1.1.1:

```
cluster1::> vserver services name-service cache hosts reverse-lookup
delete -vserver vs0 -ip 1.1.1.1
```

vserver services name-service cache hosts reverse-lookup show

Display ip-to-host struct

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

Description

The `vserver services name-service cache hosts reverse-lookup show` command displays the cached IP to host lookup(reverse lookup) entries.

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 ] }`

Use this parameter to display detailed information about the cached reverse lookup table entries.

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

Use this parameter to specify the Vserver for which the cached reverse lookup table entries need to be displayed.

[-ip <IP Address>] - IP Address (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified IP address.

[-serv-flag <integer>] - Service flags (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specifed service flag.

[-host <text>] - Hostname (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified hostname.

[-service <text>] - Service Name (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified service name.

[-aliases <text>,…] - Host Aliases (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified aliases.

[-addrtype <integer>] - Address Type (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified address type.

[-addrlength <integer>] - Address Length (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified address length.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified create time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified source.

[-ttl <integer>] - DNS TTL (privilege: advanced)

Use this parameter to display information only about the cached reverse lookup table entries that have the specified Time To Live.

Examples

The following example displays all the cached reverse lookup entries:

```
cluster1::> vserver services name-service cache hosts reverse-lookup show
```

The following example displays the cached reverse lookup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts reverse-lookup show
-vserver vs0
```

vserver services name-service cache hosts settings modify

Modify Hosts Cache Configuration

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

Description

The `vserver services name-service cache hosts settings modify` command modifies the hosts cache configuration of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the hosts cache settings need to be modified.

`[-is-enabled {true|false}]` - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the hosts database. The value *`true`* means the cache is enabled and the value *`false`* means the cache is disabled. The default value for this parameter is *`true`* .

`[-is-negative-cache-enabled {true|false}]` - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the hosts database and the lookup fails. The default value for this parameter is *`true`* . Negative cache is disabled by default if the parameter *`is-enabled`* is set to *`false`* .

`[-ttl <[<integer>h][<integer>m][<integer>s]>]` - Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the positive entries need to be cached. The positive entries means the entries which are present in the hosts database and the lookup succeeds. The default value is 24 hours.

`[-negative-ttl <[<integer>h][<integer>m][<integer>s]>]` - Negative Time to Live (privilege: advanced)

Use this parameter to specify the time for which the negative entries need to be cached. The default value is 1 minute.

`[-is-dns-ttl-enabled {true|false}]` - Is TTL Taken from DNS (privilege: advanced)

Specifies whether TTL is taken from DNS or host settings. If this parameter is true, TTL is based on the DNS setting. If false, TTL is based on the host setting. The default value is true.

Examples

The following example modifies the hosts cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts settings modify
-vserver vs0 -ttl 600 -negative-ttl 300
```

The following example disables the cache for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts settings modify
-vserver vs0 -is-enabled false
```

vserver services name-service cache hosts settings show

Display Hosts Cache Configuration

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

Description

The `vserver services name-service cache hosts settings show` command displays information about the hosts cache configuration of the 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] }

Use this parameter to display detailed information about the hosts cache configuration settings.

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

Use this parameter to display information about the hosts cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the hosts cache configuration settings that have the specified cache enabled setting. Value *`true`* displays only the entries that have cache enabled and value *`false`* displays only the entries that have cache disabled.

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the hosts cache configuration settings that have the specified negative cache enabled setting. Value *`true`* displays only the entries that have negative cache enabled and value *`false`* displays only the entries that have negative cache disabled.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to display information only about the hosts cache configuration settings that have the specified Time to Live.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to display information only about the hosts cache configuration setings that have the specified negative Time to Live.

[-is-dns-ttl-enabled {true|false}] - Is TTL Taken from DNS (privilege: advanced)

Specifies whether TTL is based on the DNS or host settings.

Examples

The following example shows the hosts cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache hosts settings show
-vserver vs0
```

The following example shows the hosts cache configuration settings that have cache disabled:

```
cluster1::> vserver services name-service cache hosts settings show -is
-enabled false
```

vserver services name-service cache netgroups ip-to-netgroup delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache netgroups ip-to-netgroup delete-all` command removes all the cached client IP to netgroup entries of the specified Vserver.

Parameters

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

Use this parameter to specify the Vserver for which the cached client IP to netgroup entries need to be deleted.

Examples

The following example deletes all the cached IP to netgroup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups ip-to-netgroup
delete-all -vserver vs0
```

vserver services name-service cache netgroups ip-to-netgroup delete

Delete netgroup.byhost cache entry

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

Description

The `vserver services name-service cache netgroups ip-to-netgroup delete` command removes the cached client IP to netgroup entries.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached client IP to netgroup entries need to be deleted.

`-host <text>` - Host field (privilege: advanced)

Use this parameter to specify the IP address for which the cached IP to netgroup entries need to be deleted.

`-netgrp <text>` - Netgroup field (privilege: advanced)

Use this parameter to specify the netgroup for which the cached IP to netgroup entries need to be deleted.

Examples

The following example deletes all the cached IP to netgroup entries for Vserver vs0, host 1.1.1.1 and netgrp 'abc':

```
cluster1::> vserver services name-service cache netgroups ip-to-netgroup
delete -vserver vs0 -host 1.1.1.1 -netgrp abc
```

vserver services name-service cache netgroups ip-to-netgroup show

Display netgroup.byhost cache entries

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

Description

The `vserver services name-service cache netgroups ip-to-netgroup show` command displays the cached client IP to netgroup entries.

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] }

Use this parameter to display detailed information about the cached client IP to netgroup entries.

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

Use this parameter to specify the Vserver for which the cached client IP to netgroup entries need to be displayed.

[-host <text>] - Host field (privilege: advanced)

Use this parameter to display information only about the cached IP to netgroup entries that have the specified IP address.

[-netgrp <text>] - Netgroup field (privilege: advanced)

Use this parameter to display information only about the cached IP to netgroup entries that have the specifed netgroup.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the IP to netgroup entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the cached IP to netgroup entries that have the specified look-up source.

Examples

The following example displays all the cached IP to netgroup entries:

```
cluster1::> vserver services name-service cache netgroups ip-to-netgroup
show
```

The following example shows all the cached IP to netgroup entries for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups ip-to-netgroup
show -vserver vs0
```

vserver services name-service cache netgroups members delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache netgroups members delete-all` command deletes all the cached netgroup member entries of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached netgroup members entries need to be deleted.

Examples

The following example deletes all the cached netgroup members of Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups members delete-
all -vserver vs0
```

vserver services name-service cache netgroups members delete

Delete netgroup cache entry

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

Description

The `vserver services name-service cache netgroups members delete` command deletes the cached members of the netgroups.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the cached netgroup members entries need to be deleted.

`-netgroup <text>` - Netgroup (privilege: advanced)

Use this parameter to specify the netgroup for which the cached netgroup members entries need to be deleted.

Examples

The following example deletes all the cached netgroup members entries for Vserver vs0 and netgroup 'abc':

```
cluster1::> vserver services name-service cache netgroups members delete
-vserver vs0 -netgroup abc
```

vserver services name-service cache netgroups members show

Display netgroup cache entries

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

Description

The `vserver services name-service cache netgroups members show` command displays the cached members of the netgroups.

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] }

Use this parameter to display detailed information about the cached members of a netgroup.

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

Use this parameter to specify the Vserver for which the cached netgroup members entries need to be displayed.

[-netgroup <text>] - Netgroup (privilege: advanced)

Use this parameter to display information only about the cached members that belong to the specified netgroup.

[-hosts <text>] - Hosts (privilege: advanced)

Use this parameter to display information only about the cached netgroups that have the specifed host as a member.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the netgroup member entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the cached netgroup member entries that have the specified look-up source.

Examples

The following example displays all the cached netgroup members entries:

```
cluster1::> vserver services name-service cache netgroups members show
```

The following example displays all the cached netgroup members entries for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups members show
-vserver vs0
```

vserver services name-service cache netgroups settings modify

Modify Netgroup Cache Configuration

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

Description

The `vserver services name-service cache netgroups settings modify` command modifies the netgroups cache configuration of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the netgroups cache settings need to be modified.

`[-is-enabled {true|false}]` - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the netgroups database. The value *`true`* means the cache is enabled and the value *`false`* means the cache is disabled. The default value for this parameter is *`true`* .

`[-is-negative-cache-enabled {true|false}]` - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the netgroups database and the look-up fails. The default value for this parameter is *`true`* . Negative cache is disabled by default if the parameter *`is-enabled`* is set to *`false`* .

`[-ttl <[<integer>h][<integer>m][<integer>s]>]` - Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the positive entries need to be cached. The positive entries means the entries which are present in the netgroups database and the look-up succeeds. The default value is 24 hours.

`[-negative-ttl <[<integer>h][<integer>m][<integer>s]>]` - Negative Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the negative entries need to be cached. The default value is 30 minutes.

`[-ttl-members <[<integer>h][<integer>m][<integer>s]>]` - TTL for netgroup members (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the netgroup members need to be cached. The default value is 24 hours.

Examples

The following example modifies the netgroups cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups settings modify
-vserver vs0 -ttl 600 -negative-ttl 300
```

The following example disables the cache for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups settings modify
-vserver vs0 -is-enabled false
```

vserver services name-service cache netgroups settings show

Display Netgroup Cache Configuration

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

Description

The `vserver services name-service cache netgroups settings show` command displays information about the netgroups cache configuration of the 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] }

Use this parameter to display detailed information about the netgroups cache configuration settings.

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

Use this parameter to display information about the netgroups cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the netgroups cache configuration settings that have the specified cache enabled setting. Value *`true`* displays only the entries that have cache enabled and value *`false`* displays only the entries that have cache disabled.

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the netgroups cache configuration settings that have the specified negative cache enabled setting. Value *`true`* displays only the entries that have negative cache enabled and value *`false`* displays only the entries that have negative cache disabled.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to display information only about the netgroups cache configuration settings that have the specified Time to Live.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to display information only about the netgroups cache configuration setings that have the specified negative Time to Live.

[-ttl-members <[<integer>h][<integer>m][<integer>s]>] - TTL for netgroup members (privilege: advanced)

Use this parameter to display information only about the netgroups cache configuration settings that have

the specified Time to Live for netgroup members.

Examples

The following example shows the netgroups cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache netgroups settings show
-vserver vs0
```

The following example shows the netgroups cache configuration settings that have cache disabled:

```
cluster1::> vserver services name-service cache netgroups settings show
-is-enabled false
```

vserver services name-service cache settings modify

Modify nameservice global cache settings

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

Description

The `vserver services name-service cache settings modify` command modifies the global name service cache configuration.

Parameters

`[-eviction-time-interval <[<integer>h][<integer>m][<integer>s]>]` - Cache Eviction Time Interval (privilege: advanced)

Use this parameter to specify the time interval after which a periodic cache eviction will happen. The default value is 4 hours.

`[-is-remote-fetch-enabled {true|false}]` - Is Remote Fetch Enabled (privilege: advanced)

Use this parameter to specify whether a node is allowed to fetch the data from a remote node or not. If the value is set as *`false`* , the node is not allowed to fetch the data from the remote node. If the value is set as *`true`* , remote fetch is allowed.

Examples

The following example modifies the global nameservice cache configuration:

```
cluster1::> vserver services name-service cache settings modify -eviction
-time-interval 1h -is-remote-fetch-enabled true
```

vserver services name-service cache settings show

Display nameservice global cache settings

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

Description

The `vserver services name-service cache settings show` command displays information about the global name service cache configuration.

Examples

The following example shows the global nameservice cache configuration:

```
cluster1::> vserver services name-service cache settings show
```

vserver services name-service cache unix-group group-by-gid delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache unix-group group-by-gid delete-all` command removes all the group entries that are cached by the group identifier or GID.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the group entries that are cached by the group identifier or GID need to be deleted.

Examples

The following example deletes all the cached group entries for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group group-by-gid
delete-all -vserver vs0
```

vserver services name-service cache unix-group group-by-gid delete

Delete an entry

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

Description

The `vserver services name-service cache unix-group group-by-gid delete` command removes the group entries that are cached by the group identifier or GID. If group cache propagation is enabled, the corresponding group-by-name cache entry will also be removed.

Parameters

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

Use this parameter to specify the Vserver for which the group entries that are cached by the group identifer or GID need to be deleted.

-gr-gid <integer> - gr_gid field (privilege: advanced)

Use this parameter to specify the group identifier or GID for which the cached entries need to be deleted.

Examples

The following example deletes all the cached group entries for Vserver vs0 and the group identifier or GID 123:

```
cluster1::> vserver services name-service cache unix-group group-by-gid
delete -vserver vs0 -gr-gid 123
```

vserver services name-service cache unix-group group-by-gid show

Display group struct

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

Description

The `vserver services name-service cache unix-group group-by-gid show` command displays the group information cached by the group identifier or GID.

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] }

Use this parameter to display detailed information about the group entries cached by the group identifier or GID.

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

Use this parameter to specify the Vserver for which the group entries that are cached by the group identifer or GID need to be displayed.

[-gr-gid <integer>] - gr_gid field (privilege: advanced)

Use this parameter to display information only about the cached group entries that have the specified group identifier or GID.

[-gr-name <text>] - gw_name field (privilege: advanced)

Use this parameter to display information only about the cached group entries that have the specified group name.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the group entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the group entries cached by the group identifier or GID that have the specified lookup source.

Examples

The following example displays all the groups which are cached by the group identifier or GID:

```
cluster1::> vserver services name-service cache unix-group group-by-id
show
```

The following example displays all the group entries cached by the group identifier or GID for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group group-by-id
show -vserver vs0
```

vserver services name-service cache unix-group group-by-name delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache unix-group group-by-name delete-all` command removes all the group entries that are cached by the group name for the specified Vserver.

Parameters

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

Use this parameter to specify the Vserver for which the group entries that are cached by group name need to be deleted.

Examples

The following example deletes all the cached group entries for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group group-by-name
delete-all -vserver vs0
```

vserver services name-service cache unix-group group-by-name delete

Delete an entry

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

Description

The `vserver services name-service cache unix-group group-by-name delete` command removes the group entries that are cached by group name. If group cache propagation is enabled, the corresponding group-by-gid cache entry will also be removed.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the group entries that are cached by group name need to be deleted.

`-gr-name <text>` - gw_name field (privilege: advanced)

Use this parameter to specify the group name for which the cached entries need to be deleted.

Examples

The following example deletes all the cached group entries for Vserver vs0 and group name abc:

```
cluster1::> vserver services name-service cache unix-group group-by-name
delete -vserver vs0 -gr-name abc
```

vserver services name-service cache unix-group group-by-name show

Display group struct

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

Description

The `vserver services name-service cache unix-group group-by-name show` command displays the group information cached by group 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 ]` }

Use this parameter to display detailed information about the group entries cached by group name.

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

Use this parameter to specify the Vserver for which the group entries that are cached by group name need to be displayed.

[-gr-name <text>] - gw_name field (privilege: advanced)

Use this parameter to display information only about the cached group entries that have the specified group name.

[-gr-gid <integer>] - gr_gid field (privilege: advanced)

Use this parameter to display information only about the cached group entries that have the specified group identifier or GID.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the group entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the group entries cached by group name that have the specified lookup source.

Examples

The following example displays all the groups which are cached by group name:

```
cluster1::> vserver services name-service cache unix-group group-by-name
show
```

The following example displays all the group entries cached by group name for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group group-by-name
show -vserver vs0
```

vserver services name-service cache unix-group settings modify

Modify UNIX Group Cache Configuration

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

Description

The `vserver services name-service cache unix-group settings modify` command modifies the groups cache configuration of the specified Vserver.

Parameters

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

Use this parameter to specify the Vserver for which the groups cache settings need to be modified.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the groups database. The value *true* means the cache is enabled and the value *false* means the cache is disabled. The default value for this parameter is *true* .

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the groups database and the lookup fails. The default value for this parameter is *true* . Negative cache is disabled by default if the parameter *is-enabled* is set to *false* .

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to specify the time(in hours, minutes and seconds) for which the positive entries need to be cached. The positive entries means the entries which are present in the groups database and the lookup succeeds. The default value is 24 hours.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to specify the time(in hours, minutes and seconds) for which the negative entries need to be cached. The default value is 5 minutes.

[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)

Use this parameter to specify whether the cached groups entries need to be propagated to the group by the group identifier or GID cache. The default value is *true* . Specify *false* to disable propagation.

Examples

The following example modifies the groups cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group settings modify
-vserver vs0 -ttl 600 -negative-ttl 300
```

The following example disables the cache for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group settings modify
-vserver vs0 -is-enabled false
```

vserver services name-service cache unix-group settings show

Display UNIX Group Cache Configuration

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

Description

The `vserver services name-service cache unix-group settings show` command displays information about the groups cache configuration of the 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] }

Use this parameter to display detailed information about the groups cache configuration settings.

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

Use this parameter to display information about the groups cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the groups cache configuration settings that have the specified cache enabled setting. The value *true* displays only the entries that have cache enabled and the value *false* displays only the entries that have cache disabled.

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the groups cache configuration settings that have the specified negative cache enabled setting. The value *true* displays only the entries that have negative cache enabled and the value *false* displays only the entries that have negative cache disabled.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to display information only about the groups cache configuration settings that have the specified Time to Live.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to display information only about the groups cache configuration setings that have the specified negative Time to Live.

[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)

Use this parameter to display information only about the groups cache configuration settings that have the specified propagation enabled setting. The value *true* displays only the entries that have the propagation of cached entries to groups by the group identifier or GID cache enabled and the value *false* displays only the entries that have the propagation of cached entries to groups by the group identifier or GID cache disabled.

Examples

The following example shows the groups cache configuration settings for all the Vservers:

```
cluster1::> vserver services name-service cache unix-group settings show
```

The following example shows the groups cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-group settings show
-vserver vs0
```

The following example shows the groups cache configuration settings that have cache disabled:

```
cluster1::> vserver services name-service cache unix-group settings show
-is-enabled false
```

vserver services name-service cache unix-user settings modify

Modify UNIX users Cache Configuration

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

Description

The `vserver services name-service cache unix-user settings modify` command modifies the users cache configuration of the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the users cache settings need to be modified.

`[-is-enabled {true|false}]` - Is Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the users database.The value *`true`* means the cache is enabled and the value *`false`* means the cache is disabled. The default value for this parameter is *`true`* .

`[-is-negative-cache-enabled {true|false}]` - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the users database and the look-up fails. The default value for this parameter is *`true`* . Negative cache is disabled by default if the parameter *`is-enabled`* is set to *`false`* .

`[-ttl <[<integer>h][<integer>m][<integer>s]>]` - Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the positive entries need to be cached. The positive entries means the entries which are present in the users database and the look-up succeeds. The default value is 24 hours.

`[-negative-ttl <[<integer>h][<integer>m][<integer>s]>]` - Negative Time to Live (privilege: advanced)

Use this parameter to specify the time (in hours, minutes and seconds) for which the negative entries need to be cached. The default value is 5 minutes.

[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)

Use this parameter to specify whether the cached users entries need to be propagated to the users by id cache. The default value is *true* . Specify *false* to disable propagation.

Examples

The following example modifies the users cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user settings modify
-vserver vs0 -ttl 600 -negative-ttl 300
```

The following example disables the cache for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user settings modify
-vserver vs0 -is-enabled false
```

vserver services name-service cache unix-user settings show

Display UNIX users Cache Configuration

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

Description

The `vserver services name-service cache unix-user settings show` command displays information about the users cache configuration of the 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] }

Use this parameter to display detailed information about the users cache configuration settings.

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

Use this parameter to display information about the users cache configuration settings for the Vserver you specify.

[-is-enabled {true|false}] - Is Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the users cache configuration settings that have the specified cache enabled setting. Value *true* displays only the entries that have cache enabled and value *false* displays only the entries that have cache disabled.

[-is-negative-cache-enabled {true|false}] - Is Negative Cache Enabled? (privilege: advanced)

Use this parameter to display information only about the users cache configuration settings that have the

specified negative cache enabled setting. Value *true* displays only the entries that have negative cache enabled and value *false* displays only the entries that have negative cache disabled.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live (privilege: advanced)

Use this parameter to display information only about the users cache configuration settings that have the specified Time to Live.

[-negative-ttl <[<integer>h][<integer>m][<integer>s]>] - Negative Time to Live (privilege: advanced)

Use this parameter to display information only about the users cache configuration setings that have the specified negative Time to Live.

[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)

Use this parameter to display information only about the users cache configuration settings that have the specified propagation enabled setting. Value *true* displays only the entries that have the propagation of cached entries to users by id cache enabled and value *false* displays only the entries that have the propagation of cached entries to users by id cache disabled.

Examples

The following example shows the users cache configuration settings for all the Vservers:

```
cluster1::> vserver services name-service cache unix-user settings show
```

The following example shows the users cache configuration settings for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user settings show
-vserver vs0
```

The following example shows the users cache configuration settings that have cache disabled:

```
cluster1::> vserver services name-service cache unix-user settings show
-is-enabled false
```

vserver services name-service cache unix-user user-by-id delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache unix-user user-by-id delete-all` command removes all the user entries that are cached by the user identifier or UID for the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the user entries that are cached by the user identifier or UID need to be deleted.

Examples

The following example deletes all the cached user entries for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user user-by-id
delete-all -vserver vs0
```

vserver services name-service cache unix-user user-by-id delete

Delete an entry

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

Description

The `vserver services name-service cache unix-user user-by-id delete` command removes the user entries that are cached by the user identifier or UID. If user cache propagation is enabled, the corresponding user-by-name cache entry will also be removed.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the user entries that are cached by the user identifier or UID need to be deleted.

`-pw-uid <integer>` - pw_uid field (privilege: advanced)

Use this parameter to specify the user identifier or UID for which the cached entries need to be deleted.

Examples

The following example deletes all the user entries cached by the user identifer or UID for Vserver vs0 and user identifier or UID 123:

```
cluster1::> vserver services name-service cache unix-user user-by-id
delete -vserver vs0 -pw-uid 123
```

vserver services name-service cache unix-user user-by-id show

Display password struct

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

Description

The `vserver services name-service cache unix-user user-by-id show` command displays the user information cached by the user identifier or UID.

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] }

Use this parameter to display detailed information about the user entries cached by the user identifier or UID.

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

Use this parameter to specify the Vserver for which the user entries that are cached by the user identifier or UID need to be displayed.

[-pw-uid <integer>] - pw_uid field (privilege: advanced)

Use this parameter to specify the user identifier or UID for which the cached entries need to be displayed.

[-pw-name <text>] - pw_name field (privilege: advanced)

Use this parameter to display information only about the cached user entries that have the specified user identifier or UID.

[-pw-gid <integer>] - pw_gid field (privilege: advanced)

Use this parameter to display information only about the cached user entries that have the specified group identifier or GID.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the user entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the user entries cached by the user identifier or UID that have the specified lookup source.

Examples

The following example displays all the users which are cached by the user identifier or UID:

```
cluster1::> vserver services name-service cache unix-user user-by-id show
```

The following example displays all the users entries cached by the user identifier or UID for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user user-by-id show
-vserver vs0
```

vserver services name-service cache unix-user user-by-name delete-all

Delete all the entries for the vserver

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

Description

The `vserver services name-service cache unix-user user-by-name delete-all` command removes all the user entries that are cached by the user name for the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the user entries that are cached by user name need to be deleted.

Examples

The following example deletes all the cached user entries for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user user-by-name
delete-all -vserver vs0
```

vserver services name-service cache unix-user user-by-name delete

Delete an entry

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

Description

The `vserver services name-service cache unix-user user-by-name delete` command removes the user entries that are cached by the user name. If user cache propagation is enabled, the corresponding user-by-id cache will also be removed.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the user entries that are cached by user name need to be deleted.

`-pw-name <text>` - pw_name field (privilege: advanced)

Use this parameter to specify the user name for which the cached entries need to be deleted.

Examples

The following example deletes all the cached user entries for Vserver vs0 and user name abc:

```
cluster1::> vserver services name-service cache unix-user user-by-name
delete -vserver vs0 -pw-name abc
```

vserver services name-service cache unix-user user-by-name show

Display password struct

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

Description

The `vserver services name-service cache unix-user user-by-name show` command displays the user information cached by the user 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] }

Use this parameter to display detailed information about the user entries cached by the user name.

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

Use this parameter to specify the Vserver for which the user entries that are cached by the user name need to be displayed.

[-pw-name <text>] - pw_name field (privilege: advanced)

Use this parameter to display information only about the cached user entries that have the specified user name.

[-pw-uid <integer>] - pw_uid field (privilege: advanced)

Use this parameter to display information only about the cached user entries that have the specified user identifier or UID.

[-pw-gid <integer>] - pw_gid field (privilege: advanced)

Use this parameter to display information only about the cached user entries that have the specified group identifier or GID.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the user entries that were cached at the specified time.

[-source {none|files|dns|nis|ldap|netgrp_byname|dc}] - Source of the Entry (privilege: advanced)

Use this parameter to display information only about the user entries cached by user name that have the specified look-up source.

Examples

The following example displays all the users which are cached by user name:

```
cluster1::> vserver services name-service cache unix-user user-by-name
show
```

The following example displays all the users entries cached by user name for Vserver vs0:

```
cluster1::> vserver services name-service cache unix-user user-by-name
show -vserver vs0
```

vserver services name-service dns check

Display validation status of a DNS configuration

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

Description

Use the `vserver services name-service dns check` command to check the status of configured DNS servers.

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 whose DNS mapping needs to be validated.

[-name-server <IP Address>] - Name Server

Use this parameter to display information only about name-servers that match the value you specify.

[-status {up|down}] - Name Server Status

Use this parameter to display information only about name-servers with a status that matches the value you specify.

[-status-details <text>] - Status Details

Use this parameter to display information only about name-servers with status details that match the value you specify.

Examples

The following example checks the DNS server mapping on the Vserver vs0:

```
cluster1::> vserver services name-service dns check -vserver vs0
Vserver          Name Server     Status  Status Details
---------------- --------------- ------- -------------------------
vs0              10.11.12.13     up      Response time (msec): 55
vs0              10.11.12.14     up      Response time (msec): 70
vs0              10.11.12.15     down    Connection refused.
```

vserver services name-service 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 name-service 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.

`[-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.

`[-is-tld-query-enabled {true|false}]` - Is TLD Query Enabled? (privilege: advanced)

Use this parameter to enable or disable top-level domain (TLD) queries. If the parameter is set to *`false`*, the resolver will not attempt to resolve a name that has no "." characters in it. The default value for this parameter is *`true`*.

[-require-source-address-match {true|false}] - Require Source and Reply IPs to Match (privilege: advanced)

Use this parameter to allow dns responses sourced from an IP that does not match where the vserver sent the request. If the parameter is set to *false* , the resolver will allow response from an IP other than the one to which the request was sent. The default value for this parameter is *true* .

[-require-packet-query-match {true|false}] - Require Packet Queries to Match (privilege: advanced)

Use this parameter to check if the query section of the reply packet is equal to that of the query packet. If the parameter is set to *false* , the resolver will not check if the query section of the reply packet is equal to that of the query packet. The default value for this parameter is *true* .

[-skip-config-validation <true>] - Skip Configuration Validation

Use this parameter to skip the DNS configuration validation.

The domain name specified with the `-domains` is validated with the following rules:

- The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_".
- The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9.
- The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9.
- The top level domain must contain only the following characters: A through Z, a through z.
- The maximum supported length is 254 characters.
- The system reserves the following names: "all", "local", and "localhost".

The hosts specified with the `-name-servers` parameter are validated to verify that each of the name servers is reachable, and is providing DNS services.

The validation fails, if the domain name is invalid, or there is no valid name server.

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 name-service dns create -vserver vs0 -domains
example.com -name-servers 192.168.0.16,192.168.0.24
```

vserver services name-service 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 name-service 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.

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 name-service dns delete -vserver vs0
```

vserver services name-service 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 name-service dns modify` command to modify an existing DNS server mapping.

To permanently remove a mapping, use the vserver services name-service 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.

`[-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.

[-is-tld-query-enabled {true|false}] - Is TLD Query Enabled? (privilege: advanced)

Use this parameter to enable or disable top-level domain (TLD) queries. If the parameter is set to *false*, the resolver will not attempt to resolve a name that has no "." characters in it. The default value for this parameter is *true*.

[-require-source-address-match {true|false}] - Require Source and Reply IPs to Match (privilege: advanced)

Use this parameter to allow dns responses sourced from an IP that does not match where the vserver sent the request. If the parameter is set to *false*, the resolver will allow response from an IP other than the one to which the request was sent.

[-require-packet-query-match {true|false}] - Require Packet Queries to Match (privilege: advanced)

Use this parameter to check if the query section of the reply packet is equal to that of the query packet. If the parameter is set to *false*, the resolver will not check if the query section of the reply packet is equal to that of the query packet.

[-skip-config-validation <true>] - Skip Configuration Validation

Use this parameter to skip the DNS configuration validation.

The domain name specified with the `-domains` is validated with the following rules:

- The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_".
- The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9.
- The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9.
- The top level domain must contain only the following characters: A through Z, a through z.
- The maximum supported length is 254 characters.
- The system reserves the following names: "all", "local", and "localhost".

The hosts specified with the `-name-servers` parameter are validated to verify that each of the name servers is reachable, and is providing DNS services.

The validation fails, if the domain name is invalid, or there is no valid name server.

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::> vserver services name-service dns modify -vserver vs0 -domains
example.com -name-servers 10.0.0.1,10.0.0.2
```

Related Links

- vserver services name-service dns delete

vserver services name-service dns show

Display DNS configuration

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

Description

The `vserver services name-service 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.

[-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.

[-is-tld-query-enabled {true|false}] - Is TLD Query Enabled? (privilege: advanced)

Use this parameter to display information only about DNS server mappings that have the specified TLD query setting.

[-require-source-address-match {true|false}] - Require Source and Reply IPs to Match (privilege: advanced)

Use this parameter to display information only about DNS server mappings that have the specified setting to require the source address of the response packet to match the address where the vserver sent the request.

[-require-packet-query-match {true|false}] - Require Packet Queries to Match (privilege: advanced)

Use this parameter to display information only about DNS server mappings that have the specified setting to require the query section of the reply packet to match that of the query packet.

Examples

The following example shows typical output from the command. Note that cluster1 uses different name servers for example.com.

```
cluster1::> vserver services name-service dns show
                                                  Name
Vserver         Domains                           Servers
--------------- --------------------------------- ----------------
vs1             example.com                       10.0.0.1,
                                                  10.0.0.2
vs2             example.com, example2.com         10.0.0.1,
                                                  10.0.0.2
vs3             example.com, example2.com         192.168.0.1,
                                                  192.168.0.2
```

vserver services name-service dns dynamic-update modify

Modify a Dynamic DNS Update Configuration

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

Description

The `vserver services name-service dns dynamic-update modify` command modifies the configuration for dynamic DNS updates for a Data Vserver.

Parameters

-vserver <vserver name> - Vserver

Use this parameter to specify the Vserver for which you want to modify the dynamic DNS update configuration.

[-is-enabled {true|false}] - Is Dynamic DNS Update Enabled?

Use this parameter with value `true` to enable the dynamic DNS update feature. This field is set to `false` by default.

[-use-secure {true|false}] - Use Secure Dynamic Update?

Use this parameter with value `true` to enable secure dynamic DNS updates. This field is set to `false` by default.

[-vserver-fqdn <text>] - Vserver FQDN to Be Used for DNS Updates

Use this parameter to modify the Vserver FQDN to be used for dynamic DNS updates.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live for DNS Updates (privilege: advanced)

Use this parameter to modify the Time to Live value for the dynamic DNS updates. The default value is set to 24 hours. The maximum supported value for TTL is 720 hours.

[-skip-fqdn-validation <true>] - Skip Vserver FQDN Validation

If the parameter is specified, the FQDN name validation is skipped.

Examples

The following example enables the dynamic DNS update feature and modifies the FQDN to be used for dynamic DNS updates for the Vserver vs1, specifying vs1.abcd.com as the new FQDN.

```
cluster1::*> vserver services name-service dns dynamic-update modify
-vserver vs1 -is-enabled true -vserver-fqdn vs1.abcd.com
```

The following example modifies the dynamic DNS updates configuration to only send secure updates to the DNS server configured for the Vserver vs1.

```
cluster1::*> vserver services name-service dns dynamic-update modify
-vserver vs1 -is-enabled true -use-secure true
```

vserver services name-service dns dynamic-update prepare-to-downgrade

Disable the Dynamic DNS update feature to be compatible with releases earlier than Data ONTAP 8.3.1

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

Description

The `vserver services name-service dns dynamic-update prepare-to-downgrade` command disables the Dynamic DNS updates on all Vservers and removes all related configurations. This command is used to prepare for downgrading the system to a release earlier than Data ONTAP 8.3.1 only.

Examples

The following example disables the dynamic DNS updates feature.

```
cluster1::*> vserver services name-service dns dynamic-update prepare-to-
downgrade
  Warning: This command will disable dynamic DNS updates on all Vservers,
remove
    all related configurations, and disable the dynamic DNS update
    feature. Use this command to prepare for downgrading the system to a
    release earlier than Data ONTAP 8.3.1 only.
  Do you want to continue? {y|n}:
```

vserver services name-service dns dynamic-update show

Display Dynamic DNS Update Configuration

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

Description

The `vserver services name-service dns dynamic-update show` command shows the dynamic DNS update configuration related to the DNS server for 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 dynamic DNS update configuration for the Vservers you specify.

[-is-enabled {true|false}] - Is Dynamic DNS Update Enabled?

Use this parameter with value `true` to display information about dynamic DNS update configurations that are active.

[-use-secure {true|false}] - Use Secure Dynamic Update?

Use this parameter with value `true` to display information about dynamic DNS update configurations that are set to send secure dynamic updates only.

[-vserver-fqdn <text>] - Vserver FQDN to Be Used for DNS Updates

Use this parameter to display information about dynamic DNS update configurations that are set to send the dynamic updates with the FQDN you have specified.

[-ttl <[<integer>h][<integer>m][<integer>s]>] - Time to Live for DNS Updates (privilege: advanced)

If you specify this parameter, the command displays dynamic DNS update configurations having the specified Time to Live value .

Examples

The following example shows all information about dynamic DNS update configurations.

```
cluster1::*> vserver services name-service dns dynamic-update show
      gupgclust-3::> dns dynamic-update show
      Vserver         Is-Enabled Use-Secure Vserver FQDN             TTL
      --------------- ---------- ---------- ------------------------
-------
      vs1             true       false      vs1.abcd.com             24h
      vs2             false      false      vs2.abcd.com             24h
      2 entries were displayed.
```

vserver services name-service dns dynamic-update record add

Adds a New DNS Resource Record

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

Description

The `vserver services name-service dns dynamic-update record add` command sends an update to add a new DNS resource record of an existing logical interface (LIF) of the Vserver to the configured DNS server.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which you want to add a resource record on the configured DNS server.

`-lif <lif-name>` - Logical Interface (privilege: advanced)

Use this parameter to specify the Logical Interface(LIF) name for which you want to add a resource record on the configured DNS server.

Examples

The following example adds a resource record entry for the Logical Interface lif1 belonging to the Vserver vs1 to the configured DNS server.

```
cluster1::*> vserver services name-service dns dynamic-update record add
-vserver vs1 -lif lif1
```

vserver services name-service dns dynamic-update record delete

Deletes a DNS Resource Record

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

Description

The `vserver services name-service dns dynamic-update record delete` command sends an update to remove an existing DNS resource record of the Logical Interface (LIF) of the Vserver from the configured DNS server.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver of which you want to delete a resource record from the configured DNS server.

{ `-lif <lif-name>` - Logical Interface (privilege: advanced)

Use this parameter to specify the Logical Interface(LIF) name whose corresponding resource record you want to remove from the configured DNS server.

| `-address <IP Address>` - IP Address (privilege: advanced) }

Use this parameter to specify the IP address of the Logical Interface whose corresponding resource record you want to remove from the configured DNS server.

Examples

The following example removes a resource record entry of the Logical Interface lif1 belonging to the Vserver vs1 from the configured DNS server.

```
cluster1::*> vserver services name-service dns dynamic-update record
delete -vserver vs1 -lif lif1
```

The following example removes a resource record entry of the Logical Interface whose address is 1.1.1.1 belonging to the Vserver vs1 from the configured DNS server.

```
cluster1::*> vserver services name-service dns dynamic-update record
delete -address 1.1.1.1 -vserver vs1
```

vserver services name-service 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 name-service 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 vserver vs1, with the hostname test.example.com and the alias test.

```
cluster1::> vserver services name-service dns hosts create -vserver vs1
-address 10.0.0.17 -hostname test.example.com -aliases test
```

vserver services name-service 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 name-service 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 vserver vs1.

```
cluster1::> vserver services name-service dns hosts delete -vserver vs1
-address 10.0.0.16

1 entry was deleted.
```

vserver services name-service 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 name-service 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 vserver vs1 so that the hostname stored in the host table entry for 10.0.0.57 is pgh.example.com.

```
cluster1::> vserver services name-service dns hosts modify -vserver -vs1
-address 10.0.0.57 -hostname pgh.example.com
1 entry was modified.
```

This example changes the host table of vserver vs1 to store the name loghost as an alternate hostname for IP address 10.0.0.5.

```
cluster1::> vserver services name-service dns hosts modify -vserver vs1
-address 10.0.0.5 -aliases loghost
1 entry was modified.
```

vserver services name-service dns hosts show

Display IP address to hostname mappings

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

Description

Use the `vserver services name-service 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.

```
cluster1::> vserver services name-service dns hosts show
Vserver    Address        Hostname        Aliases
---------- -------------- --------------- ----------------------
vs1      10.0.0.10      mail.example.com
                                          mail, mailhost, snmp
vs1      10.0.0.15      ftp.example.com ftp
vs1      10.0.0.16      www.example.com www
vs2      10.0.0.10      mail.example.com
                                          mail, mailhost, snmp
vs2      10.0.0.15      ftp.example.com ftp
vs2      10.0.0.16      www.example.com www
vs2      10.0.0.17      test.example.com
7 entries were displayed.
```

vserver services name-service getxxbyyy getaddrinfo

Gets the IP address information by using the host name.

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

Description

The ` vserver services name-service getxxbyyy getaddrinfo ` gets the IP address information by using the host name for a given Vserver. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-hostname <text>` - Host Name (privilege: advanced)

Use this parameter to specify the Host Name for which the IP address information is needed

`[-address-family {ipv4|ipv6|all}]` - Return Addresses for Family (privilege: advanced)

Use this parameter to specify the Address Family for which the IP address information is needed

`[-show-source {true|false}]` - Show Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Enable/Disable cache (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example requests address information for localhost:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -node
cluster1-01 -vserver vs1 -hostname localhost -address-family all -show
-source true -use-cache false
   Source used for Lookup: Files
   Host name: localhost
   Canonical name: localhost
   IPv4 : 127.0.0.1
   IPv6 : ::1
```

vserver services name-service getxxbyyy getgrbygid

Gets the group members by using the group identifier or GID.

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

Description

The ` vserver services name-service getxxbyyy getgrbygid ` gets the group members by using the group identifier or GID for a given Vserver. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-groupID <integer>` - Group ID (privilege: advanced)

Use this parameter to specify the GroupID for which the members are requested

`[-show-source {true|false}]` - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Use Locally-Cached Values (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

```
The following example requests group information for the given groupid
```

```
cluster1::*> vserver services name-service getxxbyyy getgrbygid -node
cluster1-01 -vserver vs1 -groupID 1
      name: daemon
      gid: 1
```

vserver services name-service getxxbyyy getgrbyname

Gets the group members by using the group name.

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

Description

The ` vserver services name-service getxxbyyy getgrbyname ` gets the group members by using the group name.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)
Use this parameter to specify the node where the lookup will be performed

`-vserver <vserver name>` - Vserver Name (privilege: advanced)
Use this parameter to specify the Vserver where the lookup will be performed

`-groupname <text>` - Group Name (privilege: advanced)
Use this parameter to specify the Group Name for which the members are requested

`[-show-source {true|false}]` - Source used for Lookup (privilege: advanced)
Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Use Locally-Cached Values (privilege: advanced)
If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example requests group information for the given group name

```
cluster1::*> vserver services name-service getxxbyyy getgrbyname -node
cluster1-01 -vserver vs1 -groupname daemon -show-source false
      name: daemon
      gid: 1
```

vserver services name-service getxxbyyy getgrlist

Gets the group list by using the user name.

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

Description

The ` vserver services name-service getxxbyyy getgrlist ` gets the list of groups to which user belongs. This command will go through all the sources configured for the group database in the name servers ns-switch configuration.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-username <text>` - User Name (privilege: advanced)

Use this parameter to retrieve the list of groups where the given user is a member

`[-use-cache <true>]` - Use Locally-Cached Values (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example requests the grouplist for the given username

```
cluster1::*> vserver services name-service getxxbyyy getgrlist -node
cluster1-01 -vserver vs1 -username root
      pw_name: root
      Groups: 5
```

vserver services name-service getxxbyyy gethostbyaddr

Gets the host information from the IP address.

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

Description

The ` vserver services name-service getxxbyyy gethostbyaddr ` gets the host name by using the IP address. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

-ipaddress <IP Address> - IP Address (privilege: advanced)

Use this parameter to specify the IPv4/IPv6 address for which the host information is needed

[-show-source {true|false}] - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

[-use-cache <true>] - Enable/Disable cache (privilege: advanced)

If set to *true* , locally-cached values will be used. The default value is *false* .

Examples

The following example requests host information for the given IP address:

```
cluster1::*> vserver services name-service getxxbyyy gethostbyaddr -node
cluster1-01 -vserver vs1 -ipaddress 127.0.0.1 -show-source false -use
-cache false
  IP address: 127.0.0.1
  Host name: localhost
```

vserver services name-service getxxbyyy gethostbyname

Gets the IP address information from host name.

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

Description

The ` vserver services name-service getxxbyyy gethostbyname ` gets the IP address by using the host name. The underlying service for doing the lookup is selected based on the configured name service switch order. When the look up happens from the hosts file, only the first IP address is returned for a host configured with multiple IP addresses.

Parameters

-node {<nodename>|local} - Node Name (privilege: advanced)

Node Use this parameter to specify the node where the lookup will be performed

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

Vserver Name Use this parameter to specify the Vserver where the lookup will be performed

-hostname <text> - Host Name (privilege: advanced)

Use this parameter to specify the Hostname for which the IP address information is requested

[-show-source {true|false}] - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

Examples

The following example requests IP Address information from the given hostname

```
cluster1::*> vserver services name-service getxxbyyy gethostbyname -node
cluster1-01 -vserver vs1 -hostname localhost -show-source false
  Host name: localhost
  Canonical name: localhost
  IPv4: 127.0.0.1
```

vserver services name-service getxxbyyy getnameinfo

Gets the name information by using the IP address.

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

Description

The ` vserver services name-service getxxbyyy getnameinfo ` gets the host and service by using the socket address. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-ipaddress <IP Address>` - IP Address (privilege: advanced)

Use this parameter to specify IPv4/IPv6 address for which the name information is requested

`[-show-source {true|false}]` - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Enable/Disable cache (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example gets the name information for the given IP Address:

```
cluster1::*> vserver services name-service getxxbyyy getnameinfo -node
cluster1-01 -vserver vs1 -ipaddress 127.0.0.1 -show-source false -use
-cache false
      IP address: 127.0.0.1
      Host name: localhost
```

vserver services name-service getxxbyyy getpwbyname

Gets the password entry by using the user name.

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

Description

The ` vserver services name-service getxxbyyy getpwbyname ` gets the password entry by using the user name. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-username <text>` - User Name (privilege: advanced)

Use this parameter to specify the Username for which the password entry is requested

`[-show-source {true|false}]` - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Enable/Disable cache (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example requests password entry from the given username:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -node
cluster1-01 -vserver vs1 -username vsadmin -show-source true -use-rbac
false -use-cache false
      Source used for lookup: Files
      pw_name: daemon
      pw_passwd: *
      pw_uid: 1, pw_gid: 1
      pw_gecos: Owner of many system processes
      pw_dir: /root
      pw_shell: /usr/sbin/nologin
```

vserver services name-service getxxbyyy getpwbyuid

Gets the password entry by using the user identifier or UID.

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

Description

The ` vserver services name-service getxxbyyy getpwbyuid ` gets the password entry by using the user identifier or UID. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-userID <integer>` - User ID (privilege: advanced)

Use this parameter to specify the UserID for whom the password entry is requested

`[-show-source {true|false}]` - Source used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

`[-use-cache <true>]` - Enable/Disable cache (privilege: advanced)

If set to *`true`* , locally-cached values will be used. The default value is *`false`* .

Examples

The following example requests password entry by using the user ID:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid  -node
cluster1-01 -vserver vs1 -userID 1001 -show-source true -use-rbac true
-use-cache false
      Source used for Lookup: Files
      pw_name: vsadmin
      pw_passwd: $1$f7b22f68$KihT1ptYqpEjcM4jfE60f0
      pw_uid: 1001
      pw_gid: 65533
      pw_gecos: User
      pw_dir: /var/home/vsadmin
      pw_shell: /sbin/ngsh
```

vserver services name-service getxxbyyy netgrpcheck

Check if a client is part of a netgroup using combined API

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

Description

The ` vserver services name-service getxxbyyy netgrpcheck ` checks if a client is part of a netgroup. The underlying service for doing the lookup is selected based on the configured name service switch order.

Parameters

`-node {<nodename>|local}` - Node Name (privilege: advanced)

Use this parameter to specify the node where the lookup will be performed

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

Use this parameter to specify the Vserver where the lookup will be performed

`-netgroup <text>` - Netgroup Name (privilege: advanced)

Use this parameter to specify the Netgroup name

`-clientIP <IP Address>` - Client IP Address (privilege: advanced)

Use this parameter to specify the Client IP for which the membership in a given netgroup needs to be checked

`[-enable-domain-search-flag {true|false}]` - Use DNS domain (privilege: advanced)

Use this parameter to use DNS domain. Default value for this field is true

`[-trust-any-source {true|false}]` - Trust any source (privilege: advanced)

Use this parameter to set trust any source parameter. Default value for this field is false

`[-show-source {true|false}]` - Source Used for Lookup (privilege: advanced)

Use this parameter to specify if source used for lookup needs to be displayed

Examples

The following example checks if the given client is part of the given netgroup:

```
cluster1::*> vserver services name-service getxxbyyy netgrpcheck -node
cluster1-01 -vserver vs1 -netgroup net1 -clientIP 10.232.98.198 -show
-source false
    10.232.98.198 is a member of net1
```

vserver services name-service ldap check

Display validation status of a LDAP configuration

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

Description

Use the `vserver services name-service ldap check` command to check the status of the LDAP 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

Use this parameter to specify the Vserver whose LDAP configuration needs to be validated.

[-client-config <text>] - Client Configuration Name

Use this parameter to specify the LDAP client configuration which is assigned to LDAP configuration for the specified Vserver.

[-ldap-status {up|down}] - LDAP Status

Use this parameter to display information only about LDAP configurations with a status that matches the value you specify.

[-ldap-status-details <text>] - LDAP Status Details

Use this parameter to display information only about LDAP configurations with a status detail that matches the value you specify.

[-ldap-dn-status-details <text>,…] - LDAP DN Status Details

Use this parameter to display information only about LDAP DN configurations with a status detail that matches the value you specify.

Examples

The following examples check the LDAP configuration on the SVM vs0:

```
cluster1::> vserver services name-service ldap check -vserver vs0
                  Vserver: vs0
Client Configuration Name: c1
              LDAP Status: up
      LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".
   LDAP DN Status Details: All the configured DNs are available.
```

```
cluster1::> vserver services name-service ldap check -vserver vs0
                  Vserver: vs0
Client Configuration Name: c1
              LDAP Status: up
      LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".
   LDAP DN Status Details: Validation of Domains specified in the LDAP
client configuration failed. Reason: bind-dn is invalid or bind
credentials are invalid. Correct the configuration and try again.
In the above example, you can correct the LDAP configuration by performing
either of the following procedures:
    -- If the bind-dn is invalid, use the "ldap client modify" command to
correct it.
    -- If the bind credentials are invalid, use the "ldap client modify-
bind-password" command to correct them.
```

vserver services name-service 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 name-service 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. A data Vserver or admin Vserver can be specified.

-client-config <text> - LDAP Client Configuration

This parameter specifies the name of the LDAP client configuration, defined under the `vserver services name-service ldap client` command, that you want to associate with the Vserver. The value of the bind-as-cifs-server parameter on this LDAP client should be false, if the CIFS server of the associated data Vserver does not exist or exists in workgroup mode.

[-skip-config-validation <true>] - Skip Configuration Validation

Use this parameter to skip the LDAP configuration validation.

The LDAP client configuration, specified by the `-client-config` parameter, that you want to associate with the Vserver is validated to verify that at least one of the LDAP servers is reachable, and is providing LDAP services.

.

The validation fails if ONTAP was unable to connect to any LDAP server with the specified `-client -config` .

Examples

The following example associates the LDAP client configuration "corp" with the Vserver "vs1":

```
cluster1::> vserver services name-service ldap create -vserver vs1 -client
-config corp
```

vserver services name-service 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 name-service ldap delete` command removes the LDAP configuration, which is an LDAP client configuration's association with a Vserver.

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. A data Vserver or admin Vserver can be specified.

Examples

The following example disassociates the current LDAP client configuration from Vserver "vs1".

```
cluster1::> vserver services name-service ldap delete -vserver vs1
```

vserver services name-service 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 name-service ldap modify` command modifies an LDAP client configuration's association with a Vserver.

> 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. A data Vserver or admin Vserver can be specified.

`[-client-config <text>]` - LDAP Client Configuration

This parameter specifies the name of the LDAP client configuration, defined under `vserver services name-service ldap client` command, that you want to associate with the Vserver. The value of the bind-as-cifs-server parameter on this LDAP client should be false if the CIFS server of the associated data Vserver does not exist or exists in workgroup mode.

`[-skip-config-validation <true>]` - Skip Configuration Validation

Use this parameter to skip the LDAP configuration validation.

The LDAP client configuration, specified by the `-client-config` parameter, that you want to associate with the Vserver is validated to verify that at least one of the LDAP servers is reachable, and is providing LDAP services.

.

The validation fails if ONTAP was unable to connect to any LDAP server with the specified `-client -config` .

Examples

The following example modifies the LDAP client configuration used by Vserver "vs1" to "corpnew":

```
cluster1::> vserver services name-service ldap modify -vserver vs1 -client
-config corpnew
```

vserver services name-service ldap show

Display LDAP configurations

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

Description

The `vserver services name-service 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. A data Vserver or admin Vserver can be specified.

[-client-config <text>] - LDAP Client Configuration

If you specify this parameter, the command displays information about LDAP configurations using the specified client.

Examples

The following example shows the LDAP configuration for Vserver "vs1":

```
cluster1::> vserver services name-service ldap show -vserver vs1
               Client
Vserver        Configuration
-------------- -------------
vs1            corp
```

vserver services name-service 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 name-service ldap client create` command creates an LDAP client configuration. A client configuration is associated with a Vserver using the `vserver services name-service ldap` commands.

Parameters

-vserver <Vserver Name> - Vserver

This parameter specifies the Vserver for which configuration is created. A data Vserver or admin Vserver can be specified.

-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.

{ -ldap-servers <text>,... - 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 `-servers` , `-ad-domain` or `-preferred-ad-servers` parameters. This parameter takes both FQDNs and IP addresses.

| -servers <IP Address>,... - (DEPRECATED)-LDAP Server List

(DEPRECATED)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 `-ldap-servers` , `-ad-domain` , `-preferred-ad-servers` or `-bind-as-cifs-server` parameters. This parameter is deprecated 9.1.0 and onwards. Use `-ldap-servers` instead.

| -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 `-ldap-servers` and `-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 LDAP binds made using this client configuration use the Vserver's CIFS server credentials. If you do not specify this parameter, and `-ad-domain` is configured, the default is `true` , otherwise the default is `false` . Note that the LDAP client always uses only sasl bind, if `-bind-as-cifs-server` is set to `true` . The `-min-bind-level` parameter is ignored in this case.

-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 name-service ldap client schema` commands.

[-port <integer>] - LDAP Server Port

This parameter specifies the port the LDAP client uses to connect to LDAP servers. Default value for port is `636` , if `-ldaps-enabled` parameter is specified as `true` . Otherwise, default value for port is `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|sasl}] - 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 `sasl` bind in case `-ad-domain` is configured, `simple` bind in case `-bind-dn` is configured, otherwise `anonymous` bind. Note that regardless of the `-min-bind-level` configured, LDAP client would always start bind mechanism in the order of `sasl` , then `simple` and lastly `anonymous` . Also, if `-bind-as-cifs-server` is set, then `-min-bind-level` is ignored, and only `sasl` will be used.

[-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 form, like "CN=user,DC=domain,DC=com" or "CN=administrator,CN=users,DC=domain,DC=com". 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 named DN entry and the entire subtree below the DN. If you do not specify this parameter, the scope is set to `subtree` by default.

[-user-dn <ldap_dn>] - User DN (privilege: advanced)

This parameter specifies the user DN, which overrides the base DN for user lookups.

To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple user or group DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-user-scope {base|onelevel|subtree}] - User Search Scope (privilege: advanced)

This parameter specifies the user search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-group-dn <ldap_dn>] - Group DN (privilege: advanced)

This parameter specifies the group DN, which overrides the base DN for group lookups.

To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple user or group DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-group-scope {base|onelevel|subtree}] - Group Search Scope (privilege: advanced)

This parameter specifies the group search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-netgroup-dn <ldap_dn>] - Netgroup DN (privilege: advanced)

This parameter specifies the netgroup DN, which overrides the base DN netgroup lookups.

> To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple netgroup DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-netgroup-scope {base|onelevel|subtree}] - Netgroup Search Scope (privilege: advanced)

This parameter specifies the netgroup search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-use-start-tls {true|false}] - Use start-tls Over LDAP Connections

This parameter specifies whether or not to use Start TLS over LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using Start TLS. Start TLS is a mechanism to provide secure communication by using the TLS/SSL protocols. If you do not specify this parameter, the default is `false` .

[-is-netgroup-byhost-enabled {true|false}] - Enable Netgroup-By-Host Lookup (privilege: advanced)

Use this parameter to enable or disable netgroup-by-host lookup. If your LDAP directory contains map structures equivalent to the netgroup.byhost map in NIS, enabling this feature greatly speeds up netgroup resolution queries over LDAP. By default this parameter is set to false.

[-netgroup-byhost-dn <ldap_dn>] - Netgroup-By-Host DN (privilege: advanced)

This parameter specifies the netgroup-by-host DN, which overrides the base DN for netgroup-by-host lookups.

> To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple netgroup DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-netgroup-byhost-scope {base|onelevel|subtree}] - Netgroup-By-Host Scope (privilege: advanced)

This parameter specifies the netgroup-by-host search scope for LDAP queries. If you do not specify this parameter, the scope is set to `subtree` by default.

[-session-security {none|sign|seal}] - Client Session Security

This parameter specifies the level of security to be used for LDAP communications. If you do not specify this parameter, the default is `none` .

LDAP Client Session Security can be one of the following:

- none - No Signing or Sealing.
- sign - Sign LDAP traffic.
- seal - Seal and Sign LDAP traffic.

[-referral-enabled {true|false}] - LDAP Referral Chasing

This parameter specifies whether LDAP referral is enabled or not.

[-group-membership-filter <text>] - Group Membership Filter (privilege: advanced)

This parameter specifies the custom LDAP search filter to be used when looking up group membership from an LDAP server. Examples of valid filters are "(cn=**99)", "(cn=1**)", "(|(cn=*22)(cn=*33))".

[-ldaps-enabled {true|false}] - Is LDAPS Enabled

This parameter specifies whether or not to use LDAPS over LDAP connections. If you do not specify this parameter, the value will be based on `port` . If `port` is mentioned as `636` , then the value will be `true` , otherwise the value will be `false` .

Examples

The following example creates an LDAP client configuration named `corp` that makes anonymous binds to `ldapserver.example.com` for Vserver `vs1` :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config corp -ldap-servers ldapserver.example.com
```

The following example creates an LDAP client configuration named `corp` that makes binds to `ldapserver.example.com` for Vserver `vs1` for bind-dn `diag` :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config corp -ldap-servers ldapserver.example.com -bind-dn diag
   Please enter password:
   Confirm password:
```

The following example creates an LDAP client configuration with multiple user DNs.

The following commands are only available in advanced mode.

```
cluster1::*> vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers ldapserver.example.com
   -user-dn "ou=People,dc=mypc,dc=example,dc=com;
ou=People1,dc=mypc1,dc=example2,dc=com"
```

The following example creates an LDAP client configuration with multiple user DNs, one of them containing a semicolon

```
cluster1::*> vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers ldapserver.example.com
   -user-dn "ou=People,dc=mypc,dc=example,dc=com;
ou=People1,dc=mypc1,dc=example2,dc=com"
```

The following example creates an LDAP client configuration with multiple user DNs, one of them containing a semicolon and a backslash.

```
cluster1::*> vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers ldapserver.example.com
   -user-dn "ou=People\;,dc=mypc,dc=example,dc=com\\;
ou=People1,dc=mypc1,dc=example2,dc=com"
```

The following example creates an LDAP client configuration with netgroup by host DN.

```
cluster1::*>vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers ldapserver.example.com
   -netgroup-byhost-dn nisMapName="netgroup.byhost",dc=rfcbis,dc=com
```

The following example creates an LDAP client configuration with ldap-servers as list of ip addresses.

```
cluster1::*>vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers 172.16.0.100,172.16.0.101
   -netgroup-byhost-dn nisMapName="netgroup.byhost",dc=rfcbis,dc=com
```

The following example creates an LDAP client configuration with ldap-servers as list of ip addresses and hostnames.

```
cluster1::*>vserver services ldap client create -vserver vs1 -client
-config corp -ldap-servers
ldapserver.example.com,172.16.0.100,172.16.0.101 -netgroup-byhost-dn
nisMapName="netgroup.byhost",dc=rfcbis,dc=com
```

vserver services name-service 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 name-service 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. A data Vserver or admin Vserver can be specified.

`-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 name-service ldap client delete -vserver vs1
-client-config corp
```

vserver services name-service 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 name-service 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. A data Vserver or admin Vserver can be specified.

`-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 name-service ldap client modify-bind-password
-client-config corp
  Please enter password:
  Confirm password:
```

vserver services name-service 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 name-service ldap client modify` command modifies an LDAP client configuration. A Vserver administrator can modify only configurations owned by the Vserver. Use the vserver services name-service ldap client modify-bind-password command to modify the bind password.

Parameters

[-vserver <Vserver Name>] - Vserver

This parameter specifies the name of the Vserver which owns the LDAP client you want to modify. A data Vserver or admin Vserver can be specified.

-client-config <text> - Client Configuration Name

This parameter specifies the name of the LDAP client configuration.

{ [-ldap-servers <text>,…] - 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 `-servers` , `-ad-domain` or `-preferred-ad-servers` parameters.

| [-servers <IP Address>,…] - (DEPRECATED)-LDAP Server List

(DEPRECATED)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 `-ldap-servers` , `-ad-domain` , `-preferred-ad-servers` or `-bind-as-cifs-server` parameters. This parameter is deprecated 9.1.0 and onwards. Use `-ldap-servers` instead.

| [-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` , `-ldap-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. Note that the LDAP client always uses only sasl bind, if `-bind-as-cifs-server` is set to `true` . The `-min-bind-level` parameter is ignored in this case.

[-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 name-service ldap client schema` commands.

[-port <integer>] - LDAP Server Port

This parameter specifies the port the LDAP client uses to connect to LDAP servers. Default value for port is `636` , if `-ldaps-enabled` parameter is specified as `true` . Otherwise, default value for port is `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|sasl}] - Minimum Bind Authentication Level

This parameter specifies the lowest acceptable level of security the LDAP client uses to bind to an LDAP server. Note that regardless of the `-min-bind-level` configured, LDAP client would always start bind mechanism in the order of `sasl` , then `simple` and lastly `anonymous` . Also, if `-bind-as-cifs-server` is set, then `-min-bind-level` is ignored, and only `sasl` will be used.

[-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 form, like "CN=user,DC=domain,DC=com" or "CN=administrator,CN=users,DC=domain,DC=com". 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 named DN entry and the entire subtree below the DN. If you do not specify this parameter, the scope is set to `subtree` by default.

[-user-dn <ldap_dn>] - User DN (privilege: advanced)

This parameter specifies the user DN, which overrides the base DN for user lookups.

> To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple user or group DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-user-scope {base|onelevel|subtree}] - User Search Scope (privilege: advanced)

This parameter specifies the user search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-group-dn <ldap_dn>] - Group DN (privilege: advanced)

This parameter specifies the group DN, which overrides the base DN for group lookups.

> To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple user or group DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-group-scope {base|onelevel|subtree}] - Group Search Scope (privilege: advanced)

This parameter specifies the group search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-netgroup-dn <ldap_dn>] - Netgroup DN (privilege: advanced)

This parameter specifies the netgroup DN, which overrides the base DN netgroup lookups.

To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple netgroup DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-netgroup-scope {base|onelevel|subtree}] - Netgroup Search Scope (privilege: advanced)

This parameter specifies the netgroup search scope. If you do not specify this parameter, the scope is set to `subtree` by default.

[-use-start-tls {true|false}] - Use start-tls Over LDAP Connections

This parameter specifies whether or not to use Start TLS over LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using Start TLS. Start TLS is a mechanism to provide secure communication by using the TLS/SSL protocols. If you do not specify this parameter, the default is `false` .

[-is-netgroup-byhost-enabled {true|false}] - Enable Netgroup-By-Host Lookup (privilege: advanced)

Use this parameter to enable or disable netgroup-by-host lookup. If your LDAP directory contains map structures equivalent to the netgroup.byhost map in NIS, enabling this feature greatly speeds up netgroup resolution over LDAP. By default this parameter is set to false.

[-netgroup-byhost-dn <ldap_dn>] - Netgroup-By-Host DN (privilege: advanced)

This parameter specifies the netgroup-by-host DN, which overrides the base DN for netgroup-by-host lookups.

To specify multiple DNs, separate multiple DN entries with semicolons (;). If you configure multiple netgroup DNs and a DN contains a semicolon, add an escape character (\) immediately before the semicolon or enclose the entire DN with quotation marks (").

[-netgroup-byhost-scope {base|onelevel|subtree}] - Netgroup-By-Host Scope (privilege: advanced)

This parameter specifies the netgroup-by-host search scope for LDAP queries. If you do not specify this parameter, the scope is set to `subtree` by default.

[-session-security {none|sign|seal}] - Client Session Security

This parameter specifies the level of security to be used for LDAP communications. If you do not specify this parameter, the default is `none` .

LDAP Client Session Security can be one of the following:

- none - No Signing or Sealing.
- sign - Sign LDAP traffic.
- seal - Seal and Sign LDAP traffic.

[-skip-config-validation <true>] - Skip Configuration Validation

Use this parameter to skip the LDAP client configuration validation.

The LDAP client configuration specified with the `-client-config` parameter is validated to verify that all the Vservers associated with this LDAP client configuration has at least one of the LDAP servers reachable, and is providing LDAP services.

The validation fails if ONTAP was unable to connect to any LDAP server with the specified `-client -config`.

[-referral-enabled {true|false}] - LDAP Referral Chasing

This parameter specifies whether LDAP referral is enabled or not.

[-group-membership-filter <text>] - Group Membership Filter (privilege: advanced)

This parameter specifies the custom LDAP search filter to be used when looking up group membership from an LDAP server. Examples of valid filters are "(cn=**99)", "(cn=1**)", "(|(cn=*22)(cn=*33))".

[-ldaps-enabled {true|false}] - Is LDAPS Enabled

This parameter specifies whether or not to use LDAPS over LDAP connections. If you do not specify this parameter, the value will be based on `port`. If `port` is mentioned as `636`, then the value will be `true`, otherwise the value will be `false`.

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::> vserver services name-service ldap client modify -client
-config corp -vserver vs1 -bind-dn administrator@example.com -min-bind
-level simple
```

The following example modifies the user DN of an existing LDAP client configuration to contain multiple DNs separated by a semicolon.

```
cluster1::> vserver services ldap client modify -client-config corp
-vserver vs1 -bind-dn administrator@example.com
            -user-dn "ou=People,dc=mypc,dc=example,dc=in;
ou=People1,dc=mypc,dc=example2,dc=com" -min-bind-level simple
```

The following example demonstrates how you can use a semicolon as a valid character in a DN instead of a separator.

```
cluster1::> vserver services ldap client modify -client-config corp
-vserver vs1 -bind-dn administrator@example.com
            -user-dn "ou=People\;,dc=mypc,dc=example,dc=com;
ou=People1,dc=mypc,dc=example2,dc=com"
```

The following example modifies an existing LDAP client configuration with multiple user DNs, one of them containing a semicolon and a backslash.

```
cluster1::> vserver services ldap client modify -client-config corp
-vserver vs1 -bind-dn administrator@example.com
            -user-dn "ou=People\;,dc=mypc,dc=example,dc=com\\;
ou=People1,dc=mypc,dc=example2,dc=com"
```

The following example modifies an existing LDAP client configuration with netgroup by host DN.

```
cluster1::*>vserver services ldap client modify -vserver vs1 -client
-config corp
            -netgroup-byhost-dn
nisMapName="netgroup.byhost",dc=rfcbis,dc=com
```

Related Links

- vserver services name-service ldap client modify-bind-password

vserver services name-service 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 name-service 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. A data Vserver or admin Vserver can be specified.

[-client-config <text>] - Client Configuration Name

If you specify this parameter, the command displays information about the LDAP client configuration you specify.

[-ldap-servers <text>,…] - LDAP Server List

If you specify this parameter, the command displays LDAP client configurations using the specified list of LDAP servers.

[-servers <IP Address>,…] - (DEPRECATED)-LDAP Server List

(DEPRECATED)-If you specify this parameter, the command displays LDAP client configurations using the specified list of LDAP 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. If the CIFS server is in workgroup mode, the value of this parameter should be false.

[-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|sasl}] - 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 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 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.

[-use-start-tls {true|false}] - Use start-tls Over LDAP Connections

This parameter specifies whether or not to use Start TLS over LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using Start TLS. Start TLS is a mechanism to provide secure communication by using the TLS/SSL protocols. If you do not specify this parameter, the default is `false` .

[-is-netgroup-byhost-enabled {true|false}] - Enable Netgroup-By-Host Lookup (privilege: advanced)

If you set this parameter to true, the command displays LDAP client configurations for which netgroup-by-host lookup is enabled.

[-netgroup-byhost-dn <ldap_dn>] - Netgroup-By-Host DN (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified netgroup-by-host DN.

[-netgroup-byhost-scope {base|onelevel|subtree}] - Netgroup-By-Host Scope (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified netgroup-by-host search scope.

[-session-security {none|sign|seal}] - Client Session Security

If this parameter is set to seal, the command displays LDAP client configurations where both signing and sealing are required for LDAP communications. If set to sign, the command displays LDAP client configurations where only signing is required for LDAP communications. If set to none, the command displays LDAP client configurations where no security is required for LDAP communications.

[-referral-enabled {true|false}] - LDAP Referral Chasing

If you specify this parameter, the command displays information about LDAP referral configurations using the specified client.

[-group-membership-filter <text>] - Group Membership Filter (privilege: advanced)

If you specify this parameter, the command displays LDAP client configurations using the specified group-membership filter.

[-ldaps-enabled {true|false}] - Is LDAPS Enabled

If you specify this parameter, the command displays LDAP client configurations using the specified value of this parameter.

Examples

The following example shows a summary of all of the LDAP client configurations available for Vserver `vs1` :

```
cluster1::> vserver services name-service ldap client show -vserver vs1
Vserver    Client        LDAP             Active Directory
Minimum
           Configuration Servers          Domain           Schema     Bind
Level
---------- ------------- ---------------- ---------------- ----------
----------
vs1        corp          ldapserver.      -                RFC-2307
anonymous
                         example.com
vs1        corpnew       172.16.0.200     -                RFC-2307
simple
```

vserver services name-service 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 name-service 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 (privilege: advanced)

This parameter specifies the Vserver for which you want to copy an existing LDAP schema template.

-schema <text> - Schema Template (privilege: advanced)

This parameter specifies the name of the existing schema template you want to copy.

-new-schema-name <text> - New Schema Template Name (privilege: advanced)

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 name-service ldap client schema copy -vserver
vs1 -schema RFC-2307 -new-schema-name corp-schema
```

vserver services name-service 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 name-service ldap client schema delete` command deletes an LDAP schema template. A Vserver administrator can only delete templates owned by the Vserver.

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 name-service ldap client schema delete
-vserver vs1 -schema corp-schema
```

vserver services name-service 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 name-service 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 name-service 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.

[-enable-rfc2307bis {true|false}] - Enable Support for Draft RFC 2307bis

This parameter specifies whether RFC 2307bis is enabled for the schema.

[-group-of-unique-names-object-class <text>] - RFC 2307bis groupOfUniqueNames Object Class

This parameter specifies the RFC 2307bis groupOfUniqueNames object class name defined by the schema. This parameter takes effect only when RFC 2307bis is enabled for the schema.

[-unique-member-attribute <text>] - RFC 2307bis uniqueMember Attribute

This parameter specifies the RFC 2307bis uniqueMember attribute name defined by the schema. This parameter takes effect only when RFC 2307bis is enabled for the schema.

[-windows-to-unix-object-class <text>] - Data ONTAP Name Mapping windowsToUnix Object Class

This parameter specifies the name mapping windowsToUnix object class name defined by the schema.

[-windows-account-attribute <text>] - Data ONTAP Name Mapping windowsAccount Attribute

This parameter specifies the name mapping windowsAccount attribute name defined by the schema.

[-windows-to-unix-attribute <text>] - Data ONTAP Name Mapping windowsToUnix Attribute

This parameter specifies the name mapping windowsToUnix attribute name defined by the schema.

[-windows-to-unix-no-domain-prefix {true|false}] - No Domain Prefix for windowsToUnix Name Mapping

This parameter specifies the name mapping windowsToUnixNoDomainPrefix setting defined by the schema.

[-nis-object-class <text>] - RFC 2307 nisObject Object Class

This parameter specifies the nisObject class name defined by the schema. This parameter takes effect only when netgroup.byhost is enabled for the vserver.

[-nis-mapname-attribute <text>] - RFC 2307 nisMapName Attribute

This parameter specifies the nisMapName attribute name defined by the schema. This parameter takes effect only when netgroup.byhost is enabled for the vserver.

[-nis-mapentry-attribute <text>] - RFC 2307 nisMapEntry Attribute

This parameter specifies the nisMapEntry attribute name defined by the schema. This parameter takes effect only when netgroup.byhost is enabled for the vserver.

Examples

The following example modifies the schema template called `corp-schema` owned by Vserver `vs1` to use `User` as the uid attribute name:

```
cluster1::> vserver services name-service ldap client schema modify
-vserver vs1 -schema corp-schema -uid-attribute User
```

Related Links

- vserver services name-service ldap client schema copy

vserver services name-service 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 name-service 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.

[-enable-rfc2307bis {true|false}] - Enable Support for Draft RFC 2307bis

If you set this parameter to true, the command displays RFC 2307bis enabled LDAP schema templates.

[-group-of-unique-names-object-class <text>] - RFC 2307bis groupOfUniqueNames Object Class

If you specify this parameter, the command displays schema templates with the specified groupOfUniqueNames object class.

[-unique-member-attribute <text>] - RFC 2307bis uniqueMember Attribute

If you specify this parameter, the command displays schema templates with the specified uniqueMember attribute.

[-windows-to-unix-object-class <text>] - Data ONTAP Name Mapping windowsToUnix Object Class

If you specify this parameter, the command displays schema templates with the specified windowsToUnix object class.

[-windows-account-attribute <text>] - Data ONTAP Name Mapping windowsAccount Attribute

If you specify this parameter, the command displays schema templates with the specified windowsAccount attribute.

[-windows-to-unix-attribute <text>] - Data ONTAP Name Mapping windowsToUnix Attribute

If you specify this parameter, the command displays schema templates with the specified windowsToUnix attribute.

[-windows-to-unix-no-domain-prefix {true|false}] - No Domain Prefix for windowsToUnix Name Mapping

If you specify this parameter, the command displays schema templates with the specified windowsToUnixNoDomainPrefix setting.

[-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.

[-nis-object-class <text>] - RFC 2307 nisObject Object Class

If you specify this parameter, the command displays schema templates with the specified nisObject attribute.

[-nis-mapname-attribute <text>] - RFC 2307 nisMapName Attribute

If you specify this parameter, the command displays schema templates with the specified nisMapName attribute.

[-nis-mapentry-attribute <text>] - RFC 2307 nisMapEntry Attribute

If you specify this parameter, the command displays schema templates with the specified nisMapEntry attribute.

Examples

The following example shows a summary of all of the default LDAP schema templates defined in the cluster:

```
cluster1::> vserver services name-service ldap client schema show
Vserver Schema Template Comment
------- ---------------
-----------------------------------------------------
cluster-node3
        MS-AD-BIS       Schema based on Active Directory Identity
Management for UNIX (read-only)
cluster-node3
        AD-IDMU         Schema based on Active Directory Identity
Management for UNIX (read-only)
cluster-node3
        AD-SFU          Schema based on Active Directory Services for UNIX
(read-only)
cluster-node3
        RFC-2307        Schema based on RFC 2307 (read-only)
4 entries were displayed.
```

vserver services name-service 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 name-service netgroup load` command loads netgroup definitions from a uniform resource identifier (URI) to a specified Vserver. You can load from a netgroup file at an FTP or a HTTP location (source URI) using the respective protocol.

Before Data ONTAP saves the new netgroup definitions, it checks that the netgroup file does not have any file structure issues, does not contain any syntax errors, and all entries comply with the following rules:

- A domain name consists of one or more labels separated by periods (.).
- A hostname is a valid domain name, IPv4 address, or IPv6 address.
- Valid characters for a label are all alphanumeric characters, underscore (_), and dash (-). A label may not begin or end with a dash.
- Valid characters for a username are all ASCII printable characters with the exception of whitespace, parentheses, and comma (,).
- Valid characters for a netgroup name are all alphanumeric characters, underscore (_), and dash (-). A

netgroup name may not begin with a dash.

- A single line in the netgroup file may not exceed 4096 characters.

If the file is found to contain errors, Data ONTAP will issue an error to that effect and netgroup definitions will not be loaded into the specified Vserver. After correcting the error, reload the netgroup file into the specified Vserver.

Parameters

`-vserver <vserver name>` - 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.

`[-foreground {true|false}]` - Load Netgroup in the Foreground

This parameter specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in foreground). When set to true, the command does not return until the operation completes.

`[-skip-hostname-validation <true>]` - Skip Hostname Validation (privilege: advanced)

If this parameter is specified, the hostname validation is skipped.

`[-skip-file-size-check <true>]` - Skip File Size Check Before Download (privilege: advanced)

If this parameter is specified, the file is downloaded without checking the file size. Use this parameter if the server does not supply the file size or does not provide an accurate value. This parameter can also be used to download a file greater than the default 5 MB size limit.

If this parameter is specified and the file is very large, the transfer may take a long time or fail due to disk space limitations.

`[-skip-file-duplicate-check <true>]` - Skip Netgroup File Duplicate Check (privilege: advanced)

If this parameter is specified, the netgroup file is downloaded even if the contents are same as the existing netgroup file. In this case, the existing file will be replaced.

Examples

The following example loads netgroup definitions into a Vserver named vs1 from the file netgroup1 at FTP location ftp://ftp.example.com:

```
cluster1::> vserver services name-service netgroup load -vserver vs1
-source ftp://ftp.example.com/netgroup1
```

vserver services name-service 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 name-service 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
- Hash value of the netgroup-by-host database
- File size of the netgroup definitions file

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 (privilege: advanced)

If you specify this parameter, the command displays the netgroup status only for the specified Vserver.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays the netgroup status only for the specified node.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Load Time (privilege: advanced)

If you specify this parameter, the command displays the 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 (privilege: advanced)

If you specify this parameter, command displays the 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.

[-hashvalue-byhost <text>] - Hash Value Byhost (privilege: advanced)

If you specify this parameter, the command displays the status only for the netgroup definitions that have the specified hash value for netgroup-by-host database. Note that the primary purpose of the command is to verify that the definitions on all nodes have the same hash value for netgroup-by-host database.

[-filesize {<integer>[KB|MB|GB|TB|PB]}] - File Size (privilege: advanced)

If you specify this parameter, the command displays the status only for the netgroup definitions that have the specified file size. Note that the primary purpose of the command is to verify that the definitions on all

nodes have the same file size, so querying on a specific file size is not useful in most cases.

Examples

The following example displays the netgroup definition status for all Vservers:

```
cluster1::*> vserver services name-service netgroup status
Vserver   Node     Load Time           Hash Value
Hash Value By-Host               File Size
--------- -------  ------------------ --------------------------------
-------------------------------- ----------
vs1
          node1    9/20/2008 16:04:55  e6cb38ec1396a280c0d2b77e3a84eda2
913a182a72aa1872495be398ebb2cd23 1.00KB
          node2    9/20/2008 16:04:53  e6cb38ec1396a280c0d2b77e3a84eda2
913a182a72aa1872495be398ebb2cd23 1.00KB
vs2
          node1    9/20/2008 16:06:26  c0d2b77e3a84eda2e6cb38ec1396a280
009321eddb45611e95d9f7f277ec0621 2.3MB
          node2    9/20/2008 16:06:27  c0d2b77e3a84eda2e6cb38ec1396a280
009321eddb45611e95d9f7f277ec0621 2.3MB
4 entries were displayed.
```

vserver services name-service netgroup file delete

Remove a local netgroup file

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

Description

The `vserver services name-service netgroup file delete` command deletes the local netgroup files for given Vservers.

Parameters

`-vserver <vserver name>` - Vserver

Use this parameter to specify the Vservers whose local netgroup file you want to delete. Separate multiple Vserver names with commas.

Examples

The following example deletes the local netgroup file for a Vserver named vs1.

```
cluster1::> vserver services netgroup file delete -vserver vs1
```

vserver services name-service netgroup file show

Display a local netgroup file

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

Description

The `vserver services netgroup file show` command displays the contents of the local netgroup file for the specified Vservers. All the entries under a given netgroup, specified in the Netgroup column of the command output, list the members of that netgroup. Each netgroup file specifies netgroups, which are sets of tuples. Each member of a netgroup is either the name of another netgroup, specified in the Member Netgroup column, or a specification of a tuple as follows: (Host, User, Domain) where Host, User, and Domain are character string names for the corresponding component. Any of the components of a tuple can either be empty to specify a wildcard value or a dash (-) to specify no valid value.

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 local netgroup file contents for the Vservers you specify.

[-netgroup <text>] - Netgroup Name

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

[-netgrpmemb <text>] - Member Netgroup

If you specify this parameter, the command displays information about the member netgroup you specify.

[-host <text>] - Member Host

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

[-user <text>] - Member User

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

[-domain <text>] - Member Domain

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

Examples

The following example displays the netgroup file contents for the Vserver named vs1.

```
cluster1::> vserver services netgroup file show -vserver vs1
                     Member
Vserver    Netgroup  Netgroup    Host           User          Domain
---------- --------  ----------- -------------- ------------
-------------------
vs1
netgrp1
                     netgrp9     -              -             -
                                 h1                           d1
                                 h22                          d22
                     netgrp11    -              -             -
                     netgrp18    -              -             -
                                 h119           u4343         d34
           netgrp8
                                 '-'            u88           '-'
```

vserver services name-service 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 name-service nis-domain create` command creates a configuration for an NIS domain. You can configure only one NIS domain for a given Vserver. 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. A data Vserver or admin Vserver can be specified.

`-domain <nis domain>` - NIS Domain

Use this parameter to specify the NIS domain for which a configuration is created. Maximum Supported NIS Domain length: 64 characters.

{ `-nis-servers <text>,…` - NIS Servers

Use this parameter to specify the hostnames/IP addresses of NIS servers used by the NIS domain configuration. Separate multiple hostnames/IP addresses with commas.

| `-servers <IP Address>,…` - (DEPRECATED)-NIS Server }

This parameter has been deprecated and might be removed in a future version of ONTAP.

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 and uses an NIS server with the IP address 192.0.2.180.

```
cluster1::> vserver services name-service nis-domain create -vserver vs0
-domain nisdomain -nis-servers 192.0.2.180
```

vserver services name-service 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 name-service nis-domain delete` command deletes an NIS domain configuration.

Deleting a NIS domain configuration removes it permanently.

Parameters

`-vserver <Vserver Name>` - Vserver

Use this parameter to specify the Vserver from which the NIS domain configuration is deleted. A data Vserver or admin Vserver can be specified.

`-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 name-service nis-domain delete -vserver vs2
-domain testnisdomain
```

vserver services name-service 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 name-service nis-domain modify` command to modify the NIS server of a NIS domain configuration.

To change the NIS domain, delete the NIS configuration using the vserver services name-service nis-domain delete command and then create the NIS configuration with new NIS domain using the vserver services name-service nis-domain create command. To permanently remove a configuration, use the vserver services name-service nis-domain delete command.

Parameters

-vserver <Vserver Name> - Vserver

Use this parameter to specify the Vserver whose NIS domain configuration is modified. A data Vserver or admin Vserver can be specified.

-domain <nis domain> - NIS Domain

Use this parameter to specify the NIS domain whose configuration is modified.

{ [-nis-servers <text>,…] - NIS Servers

Use this parameter to specify the hostnames/IP addresses of NIS servers used by the the NIS domain configuration. Separate multiple hostnames/IP addresses with commas.

| [-servers <IP Address>,…] - (DEPRECATED)-NIS Server }

This parameter has been deprecated and might be removed in a future version of ONTAP.

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 modifies the NIS servers of a NIS domain named nisdomain on a Vserver named vs0:

```
cluster1::> vserver services name-service nis-domain modify -vserver vs0
-domain nisdomain -nis-servers 192.0.2.180
```

Related Links

- vserver services name-service nis-domain delete
- vserver services name-service nis-domain create

vserver services name-service nis-domain show-bound

Display binding status of a NIS domain configuration

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

Description

The `vserver services name-service nis-domain show-bound` command displays binding 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

If you use this parameter, the command displays binding information only about the NIS domain configurations of the specified Vservers. Use this parameter with the `-domain` parameter to display binding information only about a particular NIS domain configuration on the specified Vserver. A data Vserver or admin Vserver can be specified.

[-domain <nis domain>] - NIS Domain

If you use this parameter, the command displays binding information only about the NIS domain configurations that match the specified NIS domain name. Use this parameter with the `-vserver` parameter to display binding information only about a particular Vserver on the specified NIS domain name.

[-bound-servers <IP Address>,…] - Bound NIS Servers

If you use this parameter, the command displays NIS binding information only about the specified NIS servers.

Examples

The following example displays binding information about all NIS domain configurations:

```
cluster1::> vserver services name-service nis-domain show-bound
                                    Bound
Vserver       Domain                NIS Server
------------- -------------------- -----------------
vs1           testnisdomain1       192.0.2.180,
                                    10.0.2.15
vs2           testnisdomain2       10.0.2.17
2 entries were displayed.
```

vserver services name-service 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 name-service 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. A data Vserver or admin Vserver can be specified.

[-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.

[-nis-servers <text>,…] - NIS Servers

Use this parameter to display information only about the NIS domain configurations that use the NIS servers at the hostnames/IP addresses you specify.

[-servers <IP Address>,…] - (DEPRECATED)-NIS Server

This parameter has been deprecated and might be removed in a future version of ONTAP.

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 name-service nis-domain show
Vserver       Domain        NIS Server
------------- ------------- ------------
vs1           nisdomain     192.0.2.180
vs2           nisdomain     10.0.2.15
vs3           testnisdomain 192.0.2.128, 192.0.2.180
3 entries were displayed.
```

vserver services name-service nis-domain group-database build

Build NIS group database

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

Description

The `vserver services name-service nis-domain group-database build` command rebuilds the NIS group.byuser DB for a given Vserver if NIS is added as source for group and an active nis-domain exists.

Parameters

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

Use this parameter to specify the Vserver for which NIS group.byuser DB will be rebuilt. A data Vserver can be specified.

Examples

The following example rebuilds NIS group.byuser DB for Vserver vs0.

```
cluster1::> vserver services name-service nis-domain group-database build
-vserver vs0
```

vserver services name-service nis-domain group-database status

Display NIS group database status of the local node

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

Description

The `vserver services name-service nis-domain group-database status` command displays the status of local NIS group.byuser db across a cluster. This enables you to verify that NIS group.byuser db are consistent across all nodes.

The command displays the following information:

- Vserver name
- Node name
- Last build time of NIS group.byuser db
- Hash value of the NIS group.byuser db
- File size of the NIS group.byuser db

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 (privilege: advanced)

If you specify this parameter, the command displays the NIS group.byuser db status only for the specified Vserver.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays the NIS group.byuser db status only for the specified node.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Load Time (privilege: advanced)

If you specify this parameter, the command displays the status only for the NIS group.byuser db that were built 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 extracts the db individually.

[-filesize {<integer>[KB|MB|GB|TB|PB]}] - File Size (privilege: advanced)

If you specify this parameter, the command displays the status only for the NIS group.byuser db that have the specified file size. Note that the primary purpose of the command is to verify that the definitions on all nodes have the same file size, so querying on a specific file size is not useful in most cases.

[-hashvalue <text>] - Hash Value (privilege: advanced)

If you specify this parameter, command displays the status only for the NIS group.byuser db 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 the NIS group.byuser db status for vserver vs0 :

```
cluster1::*> vserver services name-service nis-domain group-database
status -vserver vs0
Vserver   Node            Last Build Time     File Size
--------- --------------- ------------------- ----------
Hash Value
 --------------------------------
vs0
          node1           2/14/2017 11:39:56  136KB
a30b7d6d03197a7af25de72dcc4bd64f
```

vserver services name-service nis-domain netgroup-database build

Build NIS netgroup database

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

Description

The `vserver services name-service nis-domain netgroup-database build` command rebuilds the NIS netgroup.byhost database for a given Vserver if NIS is added as the source for netgroup and an active NIS domain exists.

Parameters

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

Use this parameter to specify the Vserver for which the NIS netgroup.byhost database will be rebuilt. A data Vserver can be specified.

Examples

The following example rebuilds the NIS netgroup.byhost database for Vserver vs0.

```
cluster1::> vserver services name-service nis-domain netgroup-database
build -vserver vs0
```

vserver services name-service nis-domain netgroup-database show-status

Display NIS netgroup database status of the local node

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

Description

The `vserver services name-service nis-domain netgroup-database show-status` command displays the status of local NIS netgroup.byhost databases across a cluster. This enables you to verify that NIS netgroup.byhost databases are consistent across all nodes.

The command displays the following information:

- Vserver name
- Node name
- Last build time of the NIS netgroup.byhost database
- Hash value of the NIS netgroup.byhost database
- File size of the NIS netgroup.byhost 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.

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

If you specify this parameter, the command displays the NIS netgroup.byhost database status only for the specified Vserver.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays the NIS netgroup.byhost database status only for the

specified node.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Load Time (privilege: advanced)

If you specify this parameter, the command displays the status only for the NIS netgroup.byhost databases that were built 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 extracts the databases individually.

[-filesize {<integer>[KB|MB|GB|TB|PB]}] - File Size (privilege: advanced)

If you specify this parameter, the command displays the status only for the NIS netgroup.byhost databases that have the specified file size. Note that the primary purpose of the command is to verify that the definitions on all nodes have the same file size, so querying on a specific file size is not useful in most cases.

[-hashvalue <text>] - Hash Value (privilege: advanced)

If you specify this parameter, the command displays the status only for the NIS netgroup.byhost databases 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 the NIS netgroup.byhost database status for vserver vs0 :

```
cluster1::*> vserver services name-service nis-domain netgroup-database
status -vserver vs0
Vserver   Node            Last Build Time     File Size
--------- --------------- ------------------- ----------
Hash Value
 --------------------------------
vs0
          node1           2/14/2019 11:39:56  136KB
a30b7d6d03197a7af25de72dcc4bd64f
```

vserver services name-service nis-domain netgroup-database config modify

Modify NIS netgroup database configuration

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

Description

The `vserver services name-service nis-domain netgroup-database config modify` command modifies NIS netgroup.byhost database configuration of the specified Vserver.

Parameters

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

Use this parameter to specify the Vserver for which the settings need to be modified.

[-state {enabled|disabled}] - State (privilege: advanced)

Use this parameter to enable and disable NIS netgroup.byhost databases. Default value is disabled.

[-build-interval <[<integer>h][<integer>m][<integer>s]>] - Build Interval (privilege: advanced)

Use this parameter to specify the NIS netgroup.byhost database build time interval. Default value is 24 hours and minumum value can be set to 1 hour.

Examples

The following example enables NIS netgroup.byhost database and sets the build interval to 24 hours for Vserver vs0:

```
cluster1::> vserver services name-service nis-domain netgroup-database
config modify -vserver vs0 -build-interval 24h -state enabled
```

vserver services name-service nis-domain netgroup-database config show

Display NIS netgroup database configuration

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

Description

The `vserver services name-service nis-domain netgroup-database config show` command displays NIS netgroup.byhost database 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 (privilege: advanced)

If this parameter is specified, the command displays information only about NIS netgroup.byhost databases belonging to the specified Vservers.

[-state {enabled|disabled}] - State (privilege: advanced)

If this parameter is specified, the command displays information only about NIS netgroup.byhost databases with the specified state.

[-build-interval <[<integer>h][<integer>m][<integer>s]>] - Build Interval (privilege: advanced)

If this parameter is specified, the command displays information only about NIS netgroup.byhost databases with the specified build time interval.

Examples

The following example displays the settings for Vserver vs0:

```
cluster1::> vserver services name-service nis-domain netgroup-database
config show -vserver vs0
        Vserver: vs0
 Build Interval: 30m
          State: disabled
```

vserver services name-service ns-switch create

Create a new Name Service Switch table entry

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

Description

The `vserver services name-service ns-switch create` command specifies the order in which to lookup the name service sources, for a given Vserver and name service database. Each name service database contains some information regarding hosts, group, password, netgroup or namemap. Such a database comes from one or more name service sources such as files, DNS, LDAP or NIS.

Note: The ` vserver services name-service ns-switch ` command provides the functionality of the /etc/nsswitch.conf file on UNIX systems. For more information, see the UNIX man page for nsswitch.conf(5).

Parameters

`-vserver <vserver name>` - Vserver

Use this parameter to specify the Vserver on which to create the new name service switch entry

`-database {hosts|group|passwd|netgroup|namemap}` - Name Service Switch Database

Name Service Switch Database Use this parameter to specify the name service database for which the order of the source lookup is being specified. This parameter can have the following values:

- hosts
- group
- passwd
- netgroup
- namemap

`-sources {files|dns|ldap|nis}` - Name Service Source Order

Name Service Source Order Use this parameter to specify the name service sources and the order in which to look them up for the specified Vserver and name service database. Each name service source in the list for this parameter must be one of the following:

- files
- dns

- ldap
- nis

Separate multiple name service sources with commas.

For each database specified with the `-database` parameter, one or more sources must be specified. The valid sources for each database type are shown in the following table:

```
+----------+-------------------+
| Database |  Valid Sources    |
|----------+-------------------|
| hosts    |  files, dns       |
    | group    |  files, nis, ldap |
| passwd   |  files, nis, ldap |
    | netgroup |  files, nis, ldap |
| namemap  |  files, ldap      |
+----------+-------------------+
```

+
NOTE: If "files" is not specified as the default source for the "passwd" or "group" database, ensure that default user and group entries for the 'passwd' and 'group' respectively are present in the source configured. Default entries for "passwd" database: nobody, pcuser, root, sshd, toor, daemon, operator, bin, tty, kmem, games, news, man, smmsp, mailnull, bind, proxy, uucp, pop, www, admin, diag, autosupport. Default entries for "group" database: wheel, daemon, kmem, sys, tty, operator, mail, bin, news, man, games, ftp, staff, sshd, smmsp, mailnull, guest, bind, proxy, authpf, _pflogd, _dhcp, uucp, dialer, network, audit, www, antivirus, nogroup, nobody.

+

Examples

The following example creates name service source ordering for the hosts database on a Vserver named vs0. The order of looking up the sources is specified as files followed by DNS.

```
cluster1::> vserver services name-service ns-switch create -vserver vs0
-database hosts -sources files,dns
```

The following example creates the name service source ordering for the passwd database on a Vserver named vs1. The order of looking up the sources is specified as files, NIS and LDAP.

```
cluster1::> vserver services nameservice ns-switch create -vserver vs1
-database passwd -sources files,nis,ldap
```

vserver services name-service ns-switch delete

Remove a Name Service Switch table entry

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

Description

Use the ` vserver services name-service ns-switch delete ` command to permanently remove an existing name service switch entry.

Parameters

`-vserver <vserver name>` - Vserver

Vserver Use this parameter to specify the Vserver for which to delete the name service switch entry.

`-database {hosts|group|passwd|netgroup|namemap}` - Name Service Switch Database

Name Service Switch Database Use this parameter to specify the name service database, of the Vserver, for which the name service switch entry is to be deleted. Following are the possible values for this parameter:

- hosts
- group
- passwd
- netgroup
- name_map

Examples

The following example deletes the name service switch entry for the hosts database on a Vserver named vs0.

```
cluster1::> vserver services name-service ns-switch delete -vserver vs0
-database hosts.
```

The following example deletes the name service switch entry for the group database on a Vserver named vs1.

```
cluster1::> vserver services name-service ns-switch delete -vserver vs1
-database group.
```

vserver services name-service ns-switch modify

Change a Name Service Switch table entry

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

Description

```
Use the ` vserver services name-service ns-switch modify ` command to
modify the order of looking up the name service sources, for an existing
name service switch entry.
```

Parameters

-vserver <vserver name> - Vserver

Vserver Use this parameter to specify the Vserver on which to modify the name service switch entry. A data Vserver or admin Vserver can be specified.

-database {hosts|group|passwd|netgroup|namemap} - Name Service Switch Database

Name Service Switch Database Use this parameter to specify the name service database, of the given Vserver,for which to modify the name service switch entry. Following are the possible values for this parameter:

- hosts
- group
- passwd
- netgroup
- namemap

[-sources {files|dns|ldap|nis}] - Name Service Source Order

Name Service Source Order Use this parameter to specify the name service sources and the order in whichlook up for the specified Vserver and name service database. Each name service source in the list for this parameter must be one of the following:

- files
- dns
- ldap
- nis

Separate multiple sources with commas.

For each database specified with the `-database` parameter, one or more sources must be specified. The valid sources for each database type are shown in the following table:

```
                    +----------+--------------------+
                    | Database |  Valid Sources     |
                    |----------+--------------------|
                    | hosts    |  files, dns        |
                    | group    |  files, nis, ldap  |
                    | passwd   |  files, nis, ldap  |
                    | netgroup |  files, nis, ldap  |
                    | namemap  |  files, ldap       |
                    +----------+--------------------+
```

+
NOTE: If "files" is not specified as the default source for the "passwd" or "group" database, ensure that default user and group entries for the 'passwd' and 'group' respectively are present in the source configured. Default entries for "passwd" database: nobody, pcuser, root, sshd, toor, daemon, operator, bin, tty, kmem, games, news, man, smmsp, mailnull, bind, proxy, uucp, pop, www, admin, diag, autosupport. Default entries for "group" database: wheel, daemon, kmem, sys, tty, operator, mail, bin, news, man, games, ftp, staff, sshd, smmsp, mailnull, guest, bind, proxy, authpf, _pflogd, _dhcp, uucp, dialer, network, audit, www, antivirus, nogroup, nobody.

+

Examples

The following example modifies the name service source ordering for the hosts database on a Vserver named vs0. The order of looking up the sources is changed to only DNS.

```
cluster1::> vserver services name-service ns-switch modify -vserver vs0
-database hosts -sources dns
```

The following example modifies the name service source ordering for the passwd database on a Vserver named vs1. The order of looking up the sources is changed to LDAP followed by NIS.

```
cluster1::> vserver services name-service ns-switch modify -vserver vs1
-database passwd -sources ldap,nis
```

vserver services name-service ns-switch show

Display Name Service Switch configuration

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

Description

Use the ` vserver services name-service ns-switch show ` command to display information about one or more name service switch entries. A name service switch entry provides information about the order of looking up the name service sources, for a Vserver and name service database.

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

Vserver Use this parameter to display only the name service switch entries for the Vserver you specify. A data Vserver or admin Vserver can be specified.

[-database {hosts|group|passwd|netgroup|namemap}] - Name Service Switch Database

Name Service Switch Database Use this parameter to display only the name service switch entries of the name service database type you specify. Following are the possible values for this parameter:

- hosts
- group
- passwd
- netgroup
- name_map

[-sources {files|dns|ldap|nis}] - Name Service Source Order

Name Service Source Order Use this parameter to display only name service switch entries with the specified name service source order. Each name service source in the list for this parameter must be one of the following:

- files
- dns
- ldap
- nis

Separate multiple sources with commas.

Examples

The following example shows the output of the ` vserver services name-service ns-switch show ` command.

```
cluster1::> ` vserver services name-service ns-switch show `

                                             Source
               Vserver         Database        Order
               --------------- ------------    ---------
               vs0             hosts           files,
                                               dns
               vs1             passwd          files,
                                               ldap, nis
               2 entries were displayed.
```

vserver services name-service 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 name-service 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.

[-skip-name-validation {true|false}] - Skip Name Validation

By default, Data ONTAP validates the name to ensure it complies with the following rules:

- The name contains only these valid characters: 0 through 9, A through Z, a through z, "_", ".", and "-".
- The name does not start with the character "-".
- The name does not contain "$" except as the last character.

If the parameter is set to *true* , the name validation is skipped.

Examples

The following example adds a user named tsmith to a local UNIX group named sales on a Vserver named vs0:

```
cluster1::> vserver services name-service unix-group adduser -vserver vs0
-name sales -username tsmith
```

vserver services name-service 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 name-service 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.

[-skip-name-validation {true|false}] - Skip Name Validation

By default, Data ONTAP validates the name to ensure it complies with the following rules:

- The name contains only valid characters: 0 through 9, A through Z, a through z, "_", ".", and "-"
- The name does not start with "-"
- The name does not contain "$" except as the last character

If the parameter is set to *true* , the name validation is skipped.

Examples

The following example creates a group named sales on a Vserver named vs0. The group has the ID 94.

```
cluster1::> vserver services name-service unix-group create -vserver vs0
-name sales -id 94
```

vserver services name-service 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 name-service 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 name-service unix-group delete -vserver vs0
-name testgroup
```

vserver services name-service 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 name-service 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 name-service unix-group deluser -vserver vs0
-name eng -username testuser
```

vserver services name-service 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 name-service 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. The URI scheme must be either ftp(s) or http(s)

[-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.

[-skip-name-validation {true|false}] - Skip Name Validation

By default, Data ONTAP validates the name to ensure it complies with the following rules:

- The name contains only valid characters: 0 through 9, A through Z, a through z, "_", ".", and "-"
- The name does not start with "-"
- The name does not contain "$" except as the last character

If the parameter is set to *`true`* , the name validation is skipped.

[-foreground {true|false}] - Load Unix Groups file in the Foreground

If this parameter is set to *`false`* , the operation runs as a job in the background. Otherwise, the command does not return until the operation is complete. The default value is *`true`* .

Examples

The following example loads group information from the URI ftp://ftp.example.com/groups onto a Vserver named vs0:

```
cluster1::> vserver services name-service unix-group load-from-uri
-vserver vs0 -uri ftp://ftp.example.com/groups
```

vserver services name-service 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 name-service 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::> vserver services name-service unix-group modify -vserver vs0
-group sales -id 100
```

vserver services name-service unix-group show

Display local UNIX groups

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

Description

The `vserver services name-service 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 name-service 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 name-service unix-group file show

Display local UNIX groups file

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

Description

The `vserver services name-service unix-group file show` command displays information about local UNIX groups. It displays the content as it is from the actual UNIX group file which resides in the mroot volume.

Parameters

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

If you specify this parameter, the command displays information about the local UNIX group or groups that are located on the specified Vserver.

`[-search-string <text>]` - Pattern to be searched (privilege: advanced)

If you specify this parameter and the `-vserver` parameter, the command only displays information from the UNIX group file which matches the specified parameter.

Examples

The following example displays information about all local UNIX groups belonging to a specific Vserver:

```
cluster1::> vserver services name-service unix-group file show -vserver
vs0
   Line No  File content
----------  ---------------
          1  daemon:*:1:
          2  nobody:*:65535:
          3  pcuser:*:65534:
          4  root:*:0:
```

vserver services name-service unix-group file status

Display local Unix Groups file status

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

Description

The `vserver services name-service unix-group file status` command displays the status of local UNIX group file across a cluster. This enables you to verify that UNIX group files are consistent across all nodes that back a Vserver into which UNIX group files have been loaded.

The command displays the following information:

- Vserver name
- Node name
- Load time for the UNIX group file
- Hash value of the UNIX group file
- Hash value of the UNIX group database file
- Hash value of the UNIX group byuser database file
- File size of the UNIX group file

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 (privilege: advanced)

If you specify this parameter, the command displays the UNIX group status only for the specified Vserver.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays the UNIX group status only for the specified node.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Load Time (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX group file 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 files are different on different nodes, because each node downloads the definitions from the source URI individually.

[-hashvalue <text>] - Hash Value (privilege: advanced)

If you specify this parameter, command displays the status only for the UNIX group files that have the specified hash value. Note that the primary purpose of the command is to verify that the files on all nodes have the same hash value, so querying on a specific hash value is not useful in most cases.

[-hashvalue-db-grp <text>] - Hash Value DB (privilege: advanced)

If you specify this parameter, command displays the status only for the UNIX group files that have the specified hash value for the UNIX group database. Note that the primary purpose of the command is to verify that the files on all nodes have the same hash value, so querying on a specific hash value is not useful in most cases.

[-hashvalue-db <text>] - Hash Value byuser DB (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX group files that have the specified hash value for the UNIX group byuser database. Note that the primary purpose of the command is to verify that the files on all nodes have the same hash value for UNIX group database.

[-filesize {<integer>[KB|MB|GB|TB|PB]}] - File Size (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX group files that have the specified file size. Note that the primary purpose of the command is to verify that the files on all nodes have the same file size, so querying on a specific file size is not useful in most cases.

Examples

The following example displays the UNIX group file status for all Vservers:

```
cluster1::*> vserver services name-service unix-group file status
-instance
Vserver: vs1
                Node: node1
           Load Time: 8/9/2016 19:56:25
          Hash Value: 835c7f530fb76f96c3bca00e380d36b7
       Hash Value DB: e6cb38ec1396a280c0d2b77e3a84eda2
Hash Value byuser DB: 913a182a72aa1872495be398ebb2cd23
           File Size: 58B
Vserver: vs2
                Node: node1
           Load Time: 8/9/2016 20:15:40
          Hash Value: c0d2b77e3a84eda2e6cb38ec1396a280
       Hash Value DB: 009321eddb45611e95d9f7f277ec0621
Hash Value byuser DB: 659321eddb45611e95d9f7f277ec0621
           File Size: 2.3MB
2 entries were displayed.
```

vserver services name-service unix-group max-limit modify

Change Configuration Limits for UNIX-Group

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

Description

The `vserver services name-service unix-group max-limit modify` command enables you to modify maximum UNIX groups and group-members that can be configured on the system. This allows you to set certain limits to prevent performance issues due to service configurations using excessive resources.

Parameters

`[-limit <integer>]` - System Limit (privilege: advanced)

This parameter specifies the maximum limit that you want to set for unix-group. The default setting for the limit is 32768. The supported range of values for this parameter is 0 to 65536.

Examples

The following example modifies the system-wide limit of the total number of UNIX groups and members that can be configured on the cluster.

```
vserver services name-service unix-group max-limit modify -limit 33792
```

vserver services name-service unix-group max-limit show

Display Configuration Limits for UNIX-Group

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

Description

The `vserver services name-service unix-group max-limit show` command displays information on UNIX group limits that are configurable with vserver services name-service unix-group max-limit modify command. The output will show the following:

- Limit: The configured limit on the total number of UNIX groups and group members configurable.
- Current Count: Total number of current entries for UNIX groups and group members.

Examples

The following example shows the limits and total number of current entries for UNIX group configuration:

```
cluster1::> vserver services name-service unix-group max-limit show
  (vserver services name-service unix-group max-limit show)
Limit          Current Count
-------------- --------------
400            3
```

Related Links

- vserver services name-service unix-group max-limit modify

vserver services name-service 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 name-service 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.

`[-skip-name-validation {true|false}]` - Skip Name Validation

By default, Data ONTAP validates the name to ensure it complies with the following rules:

- The name contains only valid characters: 0 through 9, A through Z, a through z, "_", ".", and "-"
- The name does not start with "-"
- The name does not contain "$" except as the last character

If the parameter is set to *`true`* , the name validation is skipped.

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 name-service unix-user create -vserver vs0 -user
tsmith -id 4219 -primary-gid 100 -full-name "Tom Smith"
```

vserver services name-service 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 name-service 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 name-service unix-user delete -vserver vs0 -user
testuser
```

vserver services name-service 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 name-service 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`*:*`home_directory`*:*`shell`*. 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. The URI scheme must be either ftp(s) or http(s).

`[-overwrite {true|false}]` - Overwrite Entries

This optionally specifies whether user information from the URI overwrites existing user information. The default setting is `false` .

`[-skip-name-validation {true|false}]` - Skip Name Validation

By default, Data ONTAP validates the name to ensure it complies with the following rules:

- The name contains only valid characters: 0 through 9, A through Z, a through z, "_", ".", and "-"
- The name does not start with "-"
- The name does not contain "$" except as the last character

If the parameter is set to *`true`* , the name validation is skipped.

`[-foreground {true|false}]` - Load Unix Users file in the Foreground

If this parameter is set to *`false`* , the operation runs as a job in the background. Otherwise, the command does not return until the operation is complete. The default value is *`true`* .

Examples

The following example loads user information from the URI ftp://ftp.example.com/users onto a Vserver named vs0:

```
node::> vserver services name-service unix-user load-from-uri -vserver vs0
-uri ftp://ftp.example.com/users
```

vserver services name-service 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 `vserver services name-service unix-user modify` command modifies a local UNIX user's ID, primary group ID, or full name.

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 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::> vserver services name-service unix-user modify -vserver vs0 -user
pjones -primary-gid 100 -full-name "Peter Jones"
```

vserver services name-service unix-user show

Display local UNIX users

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

Description

The `vserver services name-service 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::> vserver services name-service unix-user show
     User       User   Group  Full
Vserver    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 name-service unix-user file show

Display local UNIX users file

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

Description

The `vserver services name-service unix-user file show` command displays information about local UNIX users. It displays the content as it is from the actual UNIX user file which resides in the mroot volume.

Parameters

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

If you specify this parameter, the command displays information about the local UNIX user or users that are located on the specified Vserver.

`[-search-string <text>]` - Pattern to be searched (privilege: advanced)

If you specify this parameter and the `-vserver` parameter, the command only displays information from the UNIX user file which matches the specified parameter.

Examples

The following example displays information about all local UNIX users belonging to a specific Vserver:

```
cluster1::> vserver services name-service unix-user file show -vserver vs0
   Line No  File content
----------  ----------------
         1  nobody:*:65535:65535::::::
         2  pcuser:*:65534:65534::::::
         3  root:*:0:1::::::
```

vserver services name-service unix-user file status

Display local Unix Users file status

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

Description

The `vserver services name-service unix-user file status` command displays the status of local UNIX user file across a cluster. This enables you to verify that UNIX user files are consistent across all nodes that back a Vserver into which UNIX user files have been loaded.

The command displays the following information:

- Vserver name
- Node name
- Load time for the UNIX user file
- Hash value of the UNIX user file
- Hash value of the UNIX user database file
- File size of the UNIX user file

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 (privilege: advanced)

If you specify this parameter, the command displays the UNIX user status only for the specified Vserver.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays the UNIX user status only for the specified node.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Load Time (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX user file 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 files are different on different nodes, because each node downloads the definitions from the source URI individually.

[-hashvalue <text>] - Hash Value (privilege: advanced)

If you specify this parameter, command displays the status only for the UNIX user files that have the specified hash value. Note that the primary purpose of the command is to verify that the files on all nodes have the same hash value, so querying on a specific hash value is not useful in most cases.

[-hashvalue-db <text>] - Hash Value DB (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX user files that have the specified hash value for the UNIX user database. Note that the primary purpose of the command is to verify that the files on all nodes have the same hash value for UNIX user database.

[-filesize {<integer>[KB|MB|GB|TB|PB]}] - File Size (privilege: advanced)

If you specify this parameter, the command displays the status only for the UNIX user files that have the specified file size. Note that the primary purpose of the command is to verify that the files on all nodes have the same file size, so querying on a specific file size is not useful in most cases.

Examples

The following example displays the UNIX user file status for all Vservers:

```
cluster1::*> vserver services name-service unix-user file status
Vserver   Node     Load Time           Hash Value
Hash Value DB                    File Size
--------- -------  ------------------ --------------------------------
-------------------------------- ----------
vs1
          node1    5/20/2016 16:04:55  e6cb38ec1396a280c0d2b77e3a84eda2
913a182a72aa1872495be398ebb2cd23 1.00KB
          node2    5/20/2016 16:04:53  e6cb38ec1396a280c0d2b77e3a84eda2
913a182a72aa1872495be398ebb2cd23 1.00KB
vs2
          node1    5/20/2016 16:06:26  c0d2b77e3a84eda2e6cb38ec1396a280
009321eddb45611e95d9f7f277ec0621 2.3MB
          node2    5/20/2016 16:06:27  c0d2b77e3a84eda2e6cb38ec1396a280
009321eddb45611e95d9f7f277ec0621 2.3MB
4 entries were displayed.
```

vserver services name-service unix-user max-limit modify

Change Configuration Limits for UNIX-User

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

Description

The `vserver services name-service unix-user max-limit modify` command enables you to modify maximum UNIX users that can be configured on the system. This allows you to set certain limits to prevent performance issues due to service configurations using excessive resources.

Parameters

`[-limit <integer>]` - System Limit (privilege: advanced)

This parameter specifies the maximum limit that you want to set for unix-user. The default setting for the limit is 32768. The supported range of values for this parameter is 0 to 65536.

Examples

The following example modifies the system-wide limit of the total number of UNIX users that can be configured on the cluster.

```
vserver services name-service unix-user max-limit modify -limit 33792
```

vserver services name-service unix-user max-limit show

Display Configuration Limits for UNIX-User

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

Description

The `vserver services name-service unix-user max-limit show` command displays information on UNIX user limits that are configurable with vserver services name-service unix-user max-limit modify command. The output will show the following:

- Limit: The configured limit on the total number of UNIX users configurable.
- Current Count: Total number of current entries for UNIX users configuration.

Examples

The following example shows the limits and total number of current entries for UNIX user configuration:

```
cluster1::> vserver services name-service unix-user max-limit show
  (vserver services name-service unix-user max-limit show)
Limit          Current Count
-------------- --------------
400            3
```

Related Links

- vserver services name-service unix-user max-limit modify

vserver services name-service ypbind start

Start ypbind

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

Description

The `vserver services name-service ypbind start` starts the ypbind. NIS creation will fail if ypbind is stopped. This command starts ypbind on all the nodes in a cluster and is presistent across node reboots.

Examples

The following example starts ypbind:

```
vs1::> vserver services name-service ypbind start
```

vserver services name-service ypbind status

Current ypbind status

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

Description

The `vserver services name-service ypbind status` displays whether the ypbind is running or stopped.

Examples

The following example displays ypbind status:

```
vs1::> vserver services name-service ypbind status
      Status: Running
```

vserver services name-service ypbind stop

Stop ypbind

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

Description

The `vserver services name-service ypbind stop` stops the ypbind. Command fails if NIS entries are present. This command stops ypbind on all the nodes in a cluster and is persistent across node reboots.

Examples

The following example stops ypbind:

```
vs1::> vserver services name-service ypbind stop
```

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 vserver1
-user user1
Vserver: vserver1
    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

<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 vserver1 can be terminated:

```
cluster1::> vserver services ndmp kill 1000:8002 -vserver vserver1
```

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.

[-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 7,631,441(7.2M), 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 7,631,441(7.2M).

[-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-qtree-exclude-enable {true|false}] - Enable per Qtree Exclusion

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 `-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 three authentication types: challenge, plaintext and plaintext_sso. The plaintext_sso authentication type is mutually exclusive with the other authentication types. By setting the authentication type as plaintext_sso, the actual password for the user can be used to authenticate instead of having to generate an NDMP specific password. The default of this option is *challenge* . This option is persistent across reboots.

The `-option-value` for this parameter can be {challenge | plaintext | plaintext_sso | 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-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         |
| conf         | Debug configure/reconfigure          |
| dblade       | Dblade specific messages             |
| timer        | NDMP server timeout messages         |
| vldb         | VLDB service                         |
| smf          | SMF Gateway messages                 |
| common       | NDMP common state                    |
| ext          | NDMP extensions messages             |
| 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 {undef|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.

[-is-secure-control-connection-enabled {true|false}] - Is Secure Control Connection Enabled

This option enables NDMP service to accept control connections over secure sockets on TCP port 30000. This option is persistent across reboots. The default value of this option is *false* .

Examples

The following example show how to enable NDMP on a Vserver and set authorization type to plaintext :

```
cluster1::> vserver services ndmp modify -vserver vs1 -enable true
-authtype plaintext
cluster1::>
```

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.

Examples

The following example disables NDMP on a specific Vserver:

```
cluster1::> vserver services ndmp off -vserver vs1
```

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.

Examples

The following example enables NDMP service on a specific Vserver:

```
cluster1::> vserver services ndmp on -vserver vs1
```

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
- Is Secure Control Connection
- Data Backup Mode
- Data Path
- NDMP Source Address

Parameters

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

This parameter 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.

`[-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 parameter indicates whether an NDMP session is authenticated or not.

`[-data-state <component state>]` - Data State

This parameter identifies the current state of the data server's state machine.

`[-data-operation <data operation>]` - Data Operation

This parameter identifies the data server's current operation.

`[-data-halt-reason <halt reason>]` - Data Server Halt Reason

This parameter 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 parameter 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 parameter specifies the connection endpoint information for the data server's data connection.

[-data-con-port <integer>] - Data Server Connect Port

This parameter specifies the TCP/IP port that the data server will use when establishing a data connection.

[-data-bytes-processed <integer>] - Data Bytes Processed

This parameter 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 parameter field identifies the event that caused the mover state machine to enter the HALTED state.

[-mover-record-size <integer>] - Mover Record Size

This parameter represents the current mover record size in bytes.

[-mover-record-num <integer>] - Mover Record Number

This parameter represents the last tape record processed by the mover.

[-mover-bytes-moved <integer>] - Mover Bytes Moved

This parameter 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 parameter 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 parameter 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 parameter 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 parameter 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 parameter 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 parameter 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 parameter specifies the endpoint address or addresses that the mover will use when establishing a data connection.

[-mover-con-port <integer>] - Mover Connect Port

This parameter specifies the TCP/IP port that the mover will use when establishing a data connection.

[-eff-host <host type>] - Effective Host

This parameter 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.

[-is-secure-control-connection {true|false}] - Is Secure Control Connection

This parameter specifies whether the control connection is secure or not.

[-data-backup-mode <text>] - Data Backup Mode

This parameter specifies whether the mode of data backup is Dump or SMTape.

[-data-path <text>] - Data Path

This parameter specifies the path of data being backed up.

[-source-addr <text>] - NDMP Source Address

This parameter specifies the control connection IP address of the 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
  ....
   ...
  ....
   ...
```

Related Links

- 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 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 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 three authentication types: challenge, plaintext and plaintext_sso. The plaintext_sso authentication type is mutually exclusive with the other authentication types. By setting the authentication type as plaintext_sso, the actual password for the user can be used to authenticate instead of having to generate an NDMP specific password. The default of this option is *challenge* . This option is persistent across reboots.

The possible value for this parameter can be {challenge | plaintext | plaintext_sso | 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         |
| conf         | Debug configure/reconfigure          |
| dblade       | Dblade specific messages             |
| timer        | NDMP server timeout messages         |
| vldb         | VLDB service                         |
| smf          | SMF Gateway messages                 |
| common       | NDMP common state                    |
| ext          | NDMP extensions messages             |
| 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 {undef|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.

[-is-secure-control-connection-enabled {true|false}] - Is Secure Control Connection Enabled

If this parameter is specified, the command displays NDMP options for Vservers, where the value for `is-secure-control-connection-enabled` matches the specified input value.

This option enables NDMP service to accept control connections over secure sockets on TCP port 30000. This option is persistent across reboots. The default value of this option is *false*.

Examples

The following example displays NDMP options for the Vserver(s).

```
cluster1::> vserver services ndmp show

VServer       Enabled   Authentication type
------------- --------- -------------------
cluster       true      plaintext
vs1           true      plaintext
vs2           true      plaintext
3 entries were displayed.

cluster1::>
```

The following example displays detailed NDMP options for a Vserver.

```
cluster1::*> 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: 250
          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: -
Is Secure Control Connection Enabled: false
cluster1::*>
```

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
- is-secure-control-connection

- data-backup-mode
- data-path
- source-addr

| [-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.

[-is-secure-control-connection {true|false}] - Is Secure Control Connection

This parameter specifies whether the control connection is secure or not.

[-data-backup-mode <text>] - Data Backup Mode

This parameter specifies whether the mode of data backup is Dump or SMTape.

[-data-path <text>] - Data Path

This parameter specifies the path of data being backed up.

[-source-addr <text>] - NDMP Source Address

This parameter specifies the control connection IP address of the NDMP session.

Examples

The following example displays all the NDMP sessions on the cluster:

```
cluster1::> vserver services ndmp status
                      Session
     Vserver            Id
------------------   ------------
          vserver1   1000:7445
          vserver2   1000:7446
          vserver2   1000:7447
3 entries were displayed.
```

The following example shows how to display only the sessions running belonging to Vserver vserver2:

```
cluster1::> vserver services ndmp status -vserver vserver2
                      Session
     Vserver            Id
------------------   ------------
          vserver2   1000:7446
          vserver2   1000:7447
2 entries were displayed.
```

vserver services ndmp extensions modify

Modify NDMP extension status

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

Description

This command is used to enable/disable an NDMP extension in the Vserver-aware NDMP mode.

Parameters

`[-is-extension-0x2050-enabled {true|false}]` - Is Extension 0x2050 Enabled (privilege: advanced)

If this parameter is specified, the command can be used to modify the status of the extension in the Vserver-aware mode.

Examples

The following example shows how to enable NDMP extenion 0x2050 in the Vserver-aware NDMP mode of operation:

```
cluster1::> vserver services ndmp extension modify -is-extension-0x2050
-enabled true
    cluster1::>
```

vserver services ndmp extensions show

Display NDMP extension status

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

Description

This command displays whether an NDMP extension is enabled in the Vserver-aware NDMP mode or not.

Examples

The following example shows how to check the status of NDMP extension 0x2050 in a cluster :

```
cluster1::> vserver services ndmp extension show
Is Extension 0x2050 Enabled: true
cluster1::>
```

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 vserver.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

This parameter specifies the name of the Vserver.

`-session-id <text>` - Session Identifier (privilege: advanced)

This parameter specifies the NDMP session-id on which logging needs to be started.

`-filter <text>` - Level Filter (privilege: advanced)

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-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                          |
+--------------+--------------------------------------+
| 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                |
+--------------+--------------------------------------+
```

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::*> vserver services ndmp log start -vserver cluster1-01 -session
-id 1000:35512 -filter all
```

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 (privilege: advanced)

This parameter specifies the name of the Vserver.

`-session-id <text>` - Session Identifier (privilege: advanced)

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::*> vserver services ndmp log stop -vserver cluster1-01 -session
-id 1000:35512
```

vserver services ndmp restartable-backup delete

Delete an NDMP restartable backup context

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

Description

The `vserver services ndmp restartable-backup delete` command deletes an NDMP restartable backup context. The `-force` flag can be used to forcibly destroy a NDMP restartable backup context.

Parameters

-vserver <Vserver Name> - Vserver

This parameter specifies the name of the Vserver for which NDMP restartable backup context is to be deleted.

-context-id <UUID> - Context Identifier

This parameter specifies the NDMP restartable backup context ID which needs to be deleted.

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

If this parameter is specified, the context is deleted even if there are internal errors.

Examples

The following example shows how to delete an NDMP restartable backup context:

```
cluster1::> vserver services ndmp restartable-backup delete -vserver
cluster1-01 -context-id 0f8f5c44-d540-11e5-8c45-005056963504
    cluster1::>
```

vserver services ndmp restartable-backup show

Display NDMP restartable backup contexts

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

Description

The `vserver services ndmp restartable-backup show` command lists the NDMP restartbale backup contexts present in the cluster. By default it lists the following details about the context:

- Vserver Name
- Context Identifier
- Is Cleanup Pending?

A combination of parameters can be optionally supplied so as to list only those contexts which match specific conditions. A short description of each of the parameter 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 restartable backup contexts that match the specified Vserver.

[-context-id <UUID>] - Context Identifier

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for `-context-id` matches the specified input value.

This parameter specifies the UUID of NDMP restartable backup contexts.

[-volume <volume name>] - Volume Name

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for volume matches the specified input value.

This parameter specifies the volume path information

[-is-cleanup-pending {true|false}] - Is Cleanup Pending?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for `-is-cleanup-pending` matches the specified input value.

This parameter indicates whether the context is being deleted.

[-engine-type <text>] - Backup Engine Type

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for engine-type matches the specified input value.

This parameter specifies the backup engine type.

[-auto-snapshot {true|false}] - Is Snapshot Copy Auto-created?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for auto-snapshot matches the specified input value.

This parameter indicates if the Snapshot copy was created by DUMP engine.

[-no-acls {true|false}] - Is NO_ACLS Set? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for no-acls matches the specified input value.

This parameter specifies if NO_ACLS environment variable is set.

[-dump-path <text>] - Dump Path

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for dumppath matches the specified input value.

This parameter represents the correspoding local volume path which is being backed up.

[-backup-level <integer>] - Incremental Backup Level ID

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for backup-level matches the specified input value.

This parameter specifies the backup level.

[-dump-date <integer>] - Dump Date (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for dumpdate matches the specified input value.

This parameter specifies the dumpdate value in epoch.

[-base-date <integer>] - Base Date (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for basedate matches the specified input value.

This parameter specifies the basedate value in epoch.

[-update-dump-dates {true|false}] - Dump Dates Require Update? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for update-dumpdates matches the specified input value.

This parameter indicates if dumpdates needs to be updated.

[-dump-name <text>] - Dump Name

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for dumpname matches the specified input value.

This parameter indicates the name for the dump instance.

[-all-non-qtree {true|false}] - Is NON_QUOTA_QTREE Set? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for all-non-qtree matches the specified input value.

This parameter indicates if NON_QUOTA_TREE environment variable is set.

[-print-options <integer>] - Backup Log Level (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for print-options matches the specified input value.

This parameter specifies the logging level during dump.

[-last-update <integer>] - Context Last Updated Time

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for last-update matches the specified input value.

This parameter specifies the last time(in epoch) when the context was modified.

[-has-offset-map {true|false}] - Has Offset Map?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for has-offset-map matches the specified input value.

This parameter indicates if offset map is present in the backup image.

[-offset-verify {true|false}] - Offset Verify

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for offset-verify matches the specified input value.

This parameter indicates if offset map is successfully verified during backup.

[-ndmp-env-keys <text>,…] - NDMP Environment Keys (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for

ndmpenvkeys matches the specified input value.

This parameter represents the list of NDMP environment variables set during backup.

[-ndmp-env-values <text>,…] - NDMP Environment Values (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for ndmpenvvalues matches the specified input value.

This parameter represents the values set for the NDMP environment variables.

[-ndmp-env-count <integer>] - Count of NDMP Environment Variables (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for ndmpenvcount matches the specified input value.

This parameter represents the number of NDMP enviroment variables set during backup.

[-is-restartable {true|false}] - Is Context Restartable?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for is-restartable matches the specified input value.

This parameter indicates if the NDMP restartable backup context is restartable.

[-is-busy {true|false}] - Is Context Busy?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for is-busy matches the specified input value.

This parameter indicates if the NDMP restartable backup context is busy.

[-multi-subtree {true|false}] - Is MULTI_SUBTREE_NAMES Set? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for multi-subtree matches the specified input value.

This parameter indicates if the NDMP environment variable MULTI_SUBTREE_NAMES is set.

[-logical-find {true|false}] - Is LOGICAL_FIND Set? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for logical-find matches the specified input value.

This parameter indicates if the NDMP environment variable LOGICAL_FIND is set.

[-exclude-list <text>] - Is EXCLUDE Set? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for exclude-list matches the specified input value.

This parameter represents the value of the the NDMP environment variable EXCLUDE.

[-restart-pass <integer>] - Restart Pass

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for restart-pass matches the specified input value.

This parameter specifies the dump phase from which to restart.

[-backup-results <integer>] - Status of Backup

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for backup-results matches the specified input value.

This parameter specifies the status of the backup.

[-snap-name <text>] - Snapshot Copy Name

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for snap-name matches the specified input value.

This parameter specifies the name of the Snapshot copy.

[-is-dp-vol {true|false}] - Is DP Volume? (privilege: advanced)

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for is-dp-vol matches the specified input value.

This parameter indicates if the volume specified in the NDMP restartable context is of type DP.

[-context-status <integer>] - State of the Context

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for context-status matches the specified input value.

This parameter specifies the state of the NDMP restartable context.

[-is-fg-vol {true|false}] - Is FlexGroup Volume?

If this parameter is specified, the command displays NDMP restartable backup contexts where the value for is-fg-vol matches the specified input value.

This parameter indicates if the volume specified in the NDMP restartable context is a FlexGroup volume or not.

Examples

The following example displays all the NDMP restartable contexts on the cluster:

```
cluster1::> vserver services ndmp restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ ---------------
vserver1    53a6760e-d245-11e5-a33b-005056bb2685 false
vserver2    68902360-d245-11e5-a33b-005056bb2685 true
vserver2    d7b74e0d-d24c-11e5-a33b-005056bb2685 false
3 entries were displayed.
```

The following example shows how to display only the contexts belonging to Vserver vserver2:

```
cluster1::> vserver services ndmp restartable-backup show -vserver
vserver2
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ ---------------
vserver2    68902360-d245-11e5-a33b-005056bb2685 true
vserver2    d7b74e0d-d24c-11e5-a33b-005056bb2685 false
2 entries were displayed.
```

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
```

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.

```
cluster1::vserver services web> show
Vserver         Type     Service Name     Description
Enabled
--------------- -------- ---------------- ----------------------------
-------
cluster1        admin    cem              OBSOLETE
true
cluster1        admin    ontapi           Remote Administrative API
true
cluster1        admin    portal           Data ONTAP Web Services
true
                                          Portal
n6070-8         node     cem              OBSOLETE
true
n6070-8         node     ontapi           Remote Administrative API
true
n6070-8         node     portal           Data ONTAP Web Services
true
                                          Portal
n6070-8         node     spi              Service Processor
false
                                          Infrastructure
n6070-8         node     supdiag          Support Diagnostics
true
                                          Support
n6070-9         node     cem              OBSOLETE
true
n6070-9         node     ontapi           Remote Administrative API
true
n6070-9         node     portal           Data ONTAP Web Services
true
                                          Portal
n6070-9         node     spi              Service Processor
false
                                          Infrastructure
n6070-9         node     supdiag          Support Diagnostics
false
                                          Support
13 entries were displayed.
```

Related Links

- vserver services web access show

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.

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
```

Related Links

- 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.

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
```

Related Links

- 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.

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.

```
cluster1::vserver services web access> show
Vserver         Type     Service Name     Role
--------------- -------- ---------------- ----------------
cluster1        admin    cem              none
cluster1        admin    ontapi           readonly
cluster1        admin    portal           none
cluster1        admin    spi              none
cluster1        admin    supdiag          none
vs0             cluster  ontapi           admin
6 entries were displayed.

cluster1::vserver services web access>
```

Related Links

- security login show

vserver smtape commands

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.

```
cluster1::> vserver smtape break -vserver vserver0 -volume datavol
 [Job 84] Job succeeded: SnapMirror Break Succeeded
```

vserver snapdiff-rpc-server commands

vserver snapdiff-rpc-server off

Stop the SnapDiff RPC server

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

Description

The `vserver snapdiff-rpc-server off` command turns the SnapDiff RPC server off.

Parameters

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

This parameter specifies the Vserver for which you want to turn the SnapDiff RPC server off.

Examples

The following example turns the SnapDiff RPC server off for a Vserver named vs0:

```
cluster1::> vserver snapdiff-rpc-server off -vserver vs0
```

vserver snapdiff-rpc-server on

Start the SnapDiff RPC Server

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

Description

The `vserver snapdiff-rpc-server on` command turns the SnapDiff RPC server on.

Parameters

`-vserver <vserver name>` - Vserver (privilege: advanced)

This parameter specifies the Vserver for which you want to turn the SnapDiff RPC server on.

Examples

The following example enables the SnapDiff RPC server access for a Vserver named vs0:

```
cluster1::> vserver snapdiff-rpc-server on -vserver vs0
```

vserver snapdiff-rpc-server show

Display the SnapDiff RPC server configurations of Vservers

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

Description

The `vserver snapdiff-rpc-server show` command displays the state of the SnapDiff RPC server for all the 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 the configured Vservers:

- Vserver name
- Whether SnapDiff RPC server access is enabled

You can specify additional parameters to display only the information that matches those parameters. For instance, to display the information only for the Vservers that have access enabled, enter the command with the `-state` *`on`* 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 (privilege: advanced)

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

`[-state {on|off}]` - SnapDiff RPC Server state (privilege: advanced)

If you specify this parameter, the command displays information only about the specified SnapDiff RPC server state.

Examples

The following example displays information about all the Vservers with SnapDiff RPC server configured:

```
cluster1::> vserver snapdiff-rpc-server show
Vserver      SnapDiff RPC Server State
-----------    -------------------------
vs0        on
vs1        off
2 entries were displayed.
```

vserver vscan commands

vserver vscan disable

Disable Vscan on a Vserver

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

Description

The `vserver vscan disable` command disables Vscan on a Vserver.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the name of the Vserver on which you want to disable Vscan.

Examples

The following example disables Vscan on Vserver vs1.

```
cluster1::> vserver vscan disable -vserver vs1

cluster1::> vserver vscan show -vserver vs1
Vserver: vs1
Vscan Status: off
```

vserver vscan enable

Enable Vscan on a Vserver

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

Description

The `vserver vscan enable` command enables Vscan on a Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to enable Vscan. The Vscan configuration must already exist.

Examples

The following example enables Vscan on Vserver vs1.

```
cluster1::> vserver vscan enable -vserver vs1

cluster1::> vserver vscan show -vserver vs1
Vserver: vs1
Vscan Status: on
```

vserver vscan reset

Discard cached scan information

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

Description

The `vserver vscan reset` command discards the cached information of the files that have been successfully scanned. After running this command, the files are scanned again when they are accessed.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver for which you want to discard the cached information.

Examples

The following example discards the cached information of the successfully scanned files.

```
cluster1::> vserver vscan reset -vserver vs1
Warning: Running this command can cause performance degradation because
files are scanned again when they are accessed.
Do you want to continue? {y|n}: y

cluster1::>
```

vserver vscan show-events

Display Vscan events

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

Description

The `vserver vscan show-events` command displays contents of the event log, which is generated by the cluster to capture important events. If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Event type
- Event time

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- File path
- Vscan server vendor
- Vscan server version
- Disconnect reason
- Scan engine status code
- Vserver LIF used for connection
- Consecutive occurrence count

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 (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred on the specified node.

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

If you specify this parameter, the command displays information only about the events that have occurred for the specified Vserver.

[-event-time <MM/DD/YYYY HH:MM:SS>] - Event Log Time (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred at the specified time.

[-server <IP Address>] - Server (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred for the specified server.

[-event-type <event-type>] - Event Type (privilege: advanced)

If you specify this parameter, the command displays information only about the events that are of the specified event type.

[-file-path <text>] - File Path (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified file path.

[-vendor <text>] - Vscanner Vendor (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified scan-engine vendor.

[-version <text>] - Vscanner Version (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified scan-engine version.

[-disconnect-reason <reason>] - Server Disconnect Reason (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified reason of the server disconnection.

[-lif <IP Address>] - Vserver LIF Used for Connection (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified IP address, which is used for connecting clustered Data ONTAP with the Vscan server.

Examples

The following example displays all the events captured in the cluster:

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

The following example displays detailed event information about all the infected files:

```
cluster1::*> vserver vscan show-events -event-type file-infected -instance
Node: Cluster-01
                         Vserver: vs1
                 Event Log Time: 9/5/2014 11:37:38
                          Server: 192.168.1.1
                      Event Type: file-infected
                       File Path: \\1
                Vscanner Vendor: mighty master anti-evil scanner
               Vscanner Version: 1.0
       Server Disconnect Reason: -
Vserver LIF Used for Connection: 192.168.41.231
```

vserver vscan show

Display Vscan status

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

Description

The `vserver vscan show ` command displays Vscan status information of the Vservers. If you do not specify any parameters, the command displays the following information about all Vservers:

- Vserver name
- Vscan 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.

[-vserver <vserver name>] - Vserver

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

[-vscan-status {on|off}] - Vscan Status

If you specify this parameter, the command displays information only about the Vservers that have the specified status.

Examples

The following example displays the Vscan status information.

```
cluster1::> vserver vscan show
Vserver          Vscan Status
--------------   ------------
vs1              on
vs2              off
2 entries were displayed.
```

vserver vscan connection-status show-all

Display Vscan servers connection status

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

Description

The `vserver vscan connection-status show-all` command displays connection status information of the external virus-scanning servers, or "Vscan servers". If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Connection status
- Disconnect reason

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server vendor
- Vscan server version
- Privileged user
- Vscan server connected since
- Vscan server disconnected since
- Vserver LIF used for connection

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 parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

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

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-server-status <Status>] - Server Status

If you specify this parameter, the command displays information only about the Vscan servers that have the specified status.

[-server-type <Server type>] - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

[-vendor <text>] - Vscanner Vendor

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified vendor.

[-version <text>] - Vscanner Version

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified version.

[-disconnect-reason <reason>] - Server Disconnect Reason

If you specify this parameter, the command displays information only about the Vscan servers that are disconnected because of the specified reason.

[-disconnected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscanner Was Disconnected

If you specify this parameter, the command displays information only about the Vscan servers that have been disconnected since the specified time.

[-privileged-user <text>] - Privileged User Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that are connected to clustered Data ONTAP using the specified privileged user.

[-connected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscanner Was Connected

If you specify this parameter, the command displays information only about the Vscan servers that have been connected since the specified time.

[-lif <IP Address>] - Vserver LIF Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that have used the specified IP address for connecting to clustered Data ONTAP.

Examples

The following example displays connection-status information about all Vscan servers.

```
cluster1::> vserver vscan connection-status show-all
                                            Connection
Vserver     Node              Server          Status         Disconnect
Reason
----------- ----------------- --------------- -------------
-----------------
vs1         Cluster-01        1.1.1.1         disconnected   remote-closed
vs1         Cluster-01        2.2.2.2         connected      -
vs2         Cluster-01        3.3.3.3         disconnected   no-data-lif
vs2         Cluster-01        4.4.4.4         disconnected   no-data-lif
4 entries were displayed.
```

The following example displays detailed connection-status information about all Vscan servers which are connected.

```
cluster1::> vserver vscan connection-status show-all -instance
            -server-status connected
Node: Cluster-01
                            Vserver: vs1
                             Server: 2.2.2.2
                      Server Status: connected
                        Server Type: primary
                   Vscanner Vendor: XYZ
                  Vscanner Version: 1.12.2
           Server Disconnect Reason: -
  Time When Server Was Disconnected: -
Privileged User Used for Connection: cifs\u2
     Time When Server Was Connected: 6/3/2013 08:44:21
    Vserver LIF Used for Connection: 10.238.41.223
```

vserver vscan connection-status show-connected

Display connection status of connected Vscan servers

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

Description

The `vserver vscan connection-status show-connected` command displays connection status information of the connected external virus-scanning servers, or "Vscan servers". If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Vscan server vendor
- Privileged user

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server version
- Vscan server connected since
- Vserver LIF used for connection

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 parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

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

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-vendor <text>] - Vscan Server Vendor

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified vendor.

[-version <text>] - Vscan Server Version

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified version.

[-privileged-user <text>] - Privileged User Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that are connected to clustered Data ONTAP using the specified privileged user.

`[-connected-since <MM/DD/YYYY HH:MM:SS>]` - Time When Vscan Server Was Connected

If you specify this parameter, the command displays information only about the Vscan servers that have been connected since the specified time.

`[-server-type <Server type>]` - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

`[-lif <IP Address>]` - Vserver LIF Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that have used the specified IP address for connecting to clustered Data ONTAP.

Examples

The following example displays connection-status information about all connected Vscan servers.

```
cluster1::> vserver vscan connection-status show-connected
                                                                Privileged
Vserver       Node              Server           Vendor        User
------------- ----------------- ---------------- -------------
---------------
vs1           Cluster-01        1.1.1.1          ABC           cifs\u2
vs1           Cluster-01        2.2.2.2          XYZ           cifs\u2
2 entries were displayed.
```

The following example displays detailed connection-status information about connected Vscan servers which are running XYZ scan-engine.

```
cluster1::> vserver vscan connection-status show-connected -instance
-vendor XYZ
Node: Cluster-01
                            Vserver: vs1
                             Server: 2.2.2.2
                    Vscanner Vendor: XYZ
                   Vscanner Version: 1.12
Privileged User Used for Connection: cifs\u2
   Time When Vscanner Was Connected: 6/3/2013 08:44:21
                        Server Type: primary
    Vserver LIF Used for Connection: 10.238.41.223
```

vserver vscan connection-status show-not-connected

Display connection status of Vscan servers which are allowed to connect but not yet connected

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

Description

The `vserver vscan connection-status show-not-connected` command displays connection status information of the external virus-scanning servers, or "Vscan servers" that are ready to accept connection but are not yet connected. This command could be useful for troubleshooting. If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Connection status
- Disconnect reason

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server disconnected since

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 parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

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

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-server-status <Status>] - Server Status

If you specify this parameter, the command displays information only about the Vscan servers that have the specified status.

[-disconnect-reason <reason>] - Server Disconnect Reason

If you specify this parameter, the command displays information only about the Vscan servers that are disconnected because of the specified reason.

[-disconnected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscan Server Was Disconnected

If you specify this parameter, the command displays information only about the Vscan servers that have been disconnected since the specified time.

[-server-type <Server type>] - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

Examples

The following example displays connection-status information about all Vscan servers which are ready to accept connection but not yet connected.

```
cluster1::> vserver vscan connection-status show-not-connected
                                                  Connection    Disconnect
Vserver       Node              Server            Status        Reason
------------- ----------------- ----------------- -------------
---------------
vs2           Cluster-01        3.3.3.3           disconnected  invalid-
                                                                session-id
vs2           Cluster-01        4.4.4.4           disconnected  remote-
closed
2 entries were displayed.
```

The following example displays detailed connection-status information about Vscan servers which are disconnected because the connection is remotely closed.

```
cluster1::> vserver vscan connection-status show-not-connected -instance
            -disconnect-reason remote-closed
Node: Cluster-01
                            Vserver: vs2
                             Server: 4.4.4.4
                      Server Status: disconnected
           Server Disconnect Reason: remote-closed
Time When Vscanner Was Disconnected: 6/4/2013 06:51:32
                        Server Type: primary
```

vserver vscan connection-status show

Display Vscan servers connection status summary

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

Description

The `vserver vscan connection-status show` command displays connection status summary of the external virus-scanning servers, or "Vscan servers" for a Vserver. If you do not specify any parameters, the

command displays the following information for all Vservers:

- Vserver name
- Node name
- List of connected Vscan servers
- Connected count

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 parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

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

[-servers <IP Address>,…] - List of Connected Vscan Servers

If you specify this parameter, the command displays information only about the Vservers that have the specified server or servers.

[-connection-count <integer>] - Number of Connected Vscan Servers Serving the Vserver

If you specify this parameter, the command displays information only about the Vservers that have the specified connection count.

Examples

The following example displays connection-status summary for all Vservers.

```
cluster1::> vserver vscan connection-status show
                                        Connected Connected
Vserver         Node                Server-Count Servers
--------------- ------------------- ------------
-----------------------------
vs1             Cluster-01                     2 1.1.1.1, 2.2.2.2
vs2             Cluster-01                     0 -
2 entries were displayed.
```

vserver vscan on-access-policy create

Create an On-Access policy

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

Description

The `vserver vscan on-access-policy create` command creates an On-Access policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an On-Access policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the On-Access policy that you want to create. An On-Access 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 ".".

`-protocol <CIFS>` - File-Access Protocol

This parameter specifies the protocol name for which the On-Access policy will be created. Currently only CIFS is supported.

`[-filters {scan-ro-volume|scan-execute-access}]` - Filters

This parameter specifies a list of filters which can be used to define the scope of the On-Access policy more precisely. The list can include one or more of the following:

- *`scan-ro-volume`* - Enable scans for read-only volume.
- *`scan-execute-access`* - Scan only files opened with execute-access (CIFS only).

`[-scan-mandatory {on|off}]` - Mandatory Scan

This parameter specifies whether access to a file is allowed if there are no external virus-scanning servers available for virus scanning. By default, it is on.

`[-max-file-size {<integer>[KB|MB|GB|TB|PB]}]` - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning. By default, it is *`2GB`* .

`[-paths-to-exclude <File path>,…]` - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver and can be up to 255 characters long. By default, no paths are excluded. CIFS protocol based On-Access policies must use "\" as the path separator. The path can be in one of the following forms:

- *`\dir1\dir2\name`* - This would match "\dir1\dir2\name" as well as "\dir1\dir2\name...".
- *`\dir1\dir2\name\`* - This would only match "\dir1\dir2\name...".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "\vol\a b\" and "\vol\a,b\" to the `-paths-to-exclude` in the CLI, type *"\vol\a b\","\vol\a,b\"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. By default, no file extensions are excluded. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *`*`* - Matches any string, including the empty string. For example, *`mp*`* would match mp, mp3, mp4, mpeg etc.
- *`?`* - Matches any single character. For example, *`mp?`* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *`mp*`* in the CLI, type *`"mp*"`* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. By default it is *`*`* , which means all the file extensions are considered for virus scanning except those which match one of the patterns provided in `-file-ext-to-exclude` list. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *`*`* - Matches any string, including the empty string. For example, *`mp*`* would match mp, mp3, mp4, mpeg etc.
- *`?`* - Matches any single character. For example, *`mp?`* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *`mp*`* in the CLI, type *`"mp*"`* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not. By default, it is true.

Examples

The following example creates an On-Access policy.

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name test
                -protocol CIFS -scan-mandatory on -filters scan-ro-volume
-max-file-size 3GB
                -file-ext-to-exclude "mp3","txt" -file-ext-to-include
"mp*","tx*"
                -paths-to-exclude "\vol\a b\","\vol\a,b\"

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name test
Vserver: vs1
                            Policy: test
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: true
```

vserver vscan on-access-policy delete

Delete an On-Access policy

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

Description

The `vserver vscan on-access-policy delete` command deletes an On-Access policy.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the name of the Vserver from which you want to delete an On-Access policy.

`-policy-name <Policy name>` - Policy
This parameter specifies the name of the On-Access policy that you want to delete.

Examples

The following example deletes an On-Access policy.

```
cluster1::> vserver vscan on-access-policy delete -vserver vs1 -policy
-name test

cluster1::> vserver vscan on-access-policy show -vserver vs1 -policy-name
test
There are no entries matching your query.
```

vserver vscan on-access-policy disable

Disable an On-Access policy

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

Description

The `vserver vscan on-access-policy disable` command disable an On-Access policy for the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to disable an On-Access policy. The Vserver administrator can disable On-Access policies created within the scope of the Vserver and can also disable an On-Access policy created by the cluster administrator. The cluster administrator can disable On-Access policies for any Vserver.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the On-Access policy you want to disable.

Examples

The following command disable an On-Access policy on specified Vserver.

```
cluster1::> vserver vscan on-access-policy disable -vserver vs1 -policy
-name new

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                            Policy: new
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
            File-Paths Not to Scan: \vol\temp
       File-Extensions Not to Scan: txt
```

vserver vscan on-access-policy enable

Enable an On-Access policy

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

Description

The `vserver vscan on-access-policy enable` command enables an On-Access policy for the specified Vserver. Only one On-Access policy of a specific protocol can be enabled at one time.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to enable an On-Access policy. The Vserver administrator can enable On-Access policy created within the scope of the Vserver or the cluster. The cluster administrator can enable On-Access policy 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 On-Access policy you want to enable.

Examples

The following command enables an On-Access policy on specified Vserver.

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name new

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                            Policy: new
                     Policy Status: on
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
            File-Paths Not to Scan: \vol\temp
       File-Extensions Not to Scan: txt
```

vserver vscan on-access-policy modify

Modify an On-Access policy

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

Description

The `vserver vscan on-access-policy modify` command modifies an On-Access policy.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the name of the Vserver on which you want to modify an On-Access policy.

`-policy-name <Policy name>` - Policy
This parameter specifies the name of the On-Access policy that you want to modify.

`[-filters {scan-ro-volume|scan-execute-access}]` - Filters
This parameter specifies a list of filters which can be used to define the scope of the On-Access policy more precisely. The list can include one or more of the following:

- *`scan-ro-volume`* - Enable scans for read-only volume.
- *`scan-execute-access`* - Scan only files opened with execute-access (CIFS only).

`[-scan-mandatory {on|off}]` - Mandatory Scan
This parameter specifies whether access to a file is allowed if there are no external virus-scanning servers available for virus scanning.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver and can be up to 255 characters long. CIFS protocol based On-Access policies must use "\" as the path separator. The path can be in one of the following forms:

- *\dir1\dir2\name* - This would match "\dir1\dir2\name" as well as "\dir1\dir2\name...".
- *\dir1\dir2\name* - This would only match "\dir1\dir2\name...".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "\vol\a b\" and "\vol\a,b\" to the `-paths-to-exclude` in the CLI, type *"\vol\a b\","\vol\a,b\"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not.

Examples

The following example modifies an On-Access policy.

```
cluster1::> vserver vscan on-access-policy modify -vserver vs1 -policy
-name test
                -protocol CIFS -scan-mandatory on -filters scan-ro-volume
-max-file-size 10GB
                -file-ext-to-exclude "mp3" -file-ext-to-include "mp*"
-scan-files-with-no-ext false
                -paths-to-exclude "\vol1\temp","\vol2\a"

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name test
Vserver: vs1
                            Policy: test
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: off
Max File Size Allowed for Scanning: 10GB
            File Paths Not to Scan: \vol1\temp, \vol2\a
       File Extensions Not to Scan: mp3
           File Extensions to Scan: mp*
      Scan Files with No Extension: false
```

vserver vscan on-access-policy show

Display On-Access policies

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

Description

The `vserver vscan on-access-policy show` command displays information about the On-Access policies belonging to the Vserver. It also displays the current status in Vserver scope. If you do not specify any parameters, the command displays the following information about all On-Access policies:

- Vserver name
- Policy name
- Policy status
- Policy owner

- Protocol
- File paths to exclude
- File extensions to exclude

You can specify the `-fields` parameter to specify which fields of information to display about On-Access policies. In addition to the fields above, you can display the following fields:

- List of filters
- Mandatory scan
- Max file size
- File extensions to include
- Scan files without extension

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 On-Access policies for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified On-Access policy.

[-policy-status {on|off}] - Policy Status

If you specify this parameter, the command displays information only about the On-Access policies that have the specified status.

[-owner <Configuration owner>] - Policy Config Owner

If you specify this parameter, the command displays information only about the On-Access policies that have the specified owner.

[-protocol <CIFS>] - File-Access Protocol

If you specify this parameter, the command displays information only about the On-Access policies that have the specified protocol.

[-filters {scan-ro-volume|scan-execute-access}] - Filters

If you specify this parameter, the command displays information only about the On-Access policies that have the specified filter or filters in the filter list.

[-scan-mandatory {on|off}] - Mandatory Scan

If you specify this parameter, the command displays information only about the On-Access policies that have mandatory scanning enabled.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

If you specify this parameter, the command displays information only about the On-Access policies that have the specified max-file-size.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified path or paths in the exclude list.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified file extension or extensions in the exclude list.

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified file extension or extensions in the include list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

If you specify this parameter, the command displays information only about the On-Access policies that have the specified value.

Examples

The following example displays information about all On-Access policies.

```
cluster1::> vserver vscan on-access-policy show
            Policy     Policy                              File-Ext
Policy
Vserver     Name       Owner    Protocol Paths Excluded    Excluded
Status
----------- ---------  -------- -------- ----------------- -----------
------
Cluster     default_   cluster  CIFS     -                 -           off
            CIFS
vs1         default_   cluster  CIFS     -                 -           on
            CIFS
vs1         new        vserver  CIFS     \vol\temp         txt         off
vs2         default_   cluster  CIFS     -                 -           on
            CIFS
4 entries were displayed.
```

The following example displays detailed information about an On-Access policy.

```
cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                             Policy: new
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
             File Paths Not to Scan: \vol\temp
       File Extensions Not to Scan: txt
           File Extensions to Scan: *
      Scan Files with No Extension: true
```

vserver vscan on-access-policy file-ext-to-exclude add

Add to the list of file extensions to exclude

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

Description

The `vserver vscan on-access-policy file-ext-to-exclude add` command adds a file extension or a list of file extensions that must be excluded from scanning to the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a file extension or a list of file extensions that must be excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a file extension or a list of file extensions that must be excluded from scanning.

`-file-ext-to-exclude <File extension>,…` - File Extensions Not to Scan

This parameter specifies the file extension or a list of file extensions that must be excluded from scanning.

Examples

The following example adds a list of file extensions that must be excluded from scanning to the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude add
-vserver vs1
            -policy-name policy1 -file-ext-to-exclude txt,mp4

cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
File-Extensions Not to Scan: mp3, mp4, txt, wav
```

vserver vscan on-access-policy file-ext-to-exclude remove

Remove from the list of file extensions to exclude

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

Description

The `vserver vscan on-access-policy file-ext-to-exclude remove` command removes a file extension or a list of file extensions that are excluded from scanning from the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a file extension or a list of file extensions that are excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a file extension or a list of file extensions that are excluded from scanning.

`-file-ext-to-exclude <File extension>,…` - File Extensions Not to Scan

This parameter specifies the file extension or a list of file extensions that must be removed from the on-access policy.

Examples

The following example removes a list of file extensions that are to be excluded from scanning from the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude remove
-vserver vs1
            -policy-name policy1 -file-ext-to-exclude mp3,txt

cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
File-Extensions Not to Scan: mp4, wav
```

vserver vscan on-access-policy file-ext-to-exclude show

Display list of file extensions to exclude

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

Description

The `vserver vscan on-access-policy file-ext-to-exclude show` command displays the list of file extensions that are excluded from scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on-access policies:

- Vserver name
- Policy name
- List of File-Extensions to exclude

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 policy names for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified policy name.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the policies that have the specified file extensions that are excluded from scanning.

Examples

The following example displays the list of file extensions that are excluded from scanning for all the policies:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
Vserver         Policy Name       File-Ext Excluded
--------------- -----------------
-----------------------------------------
cluster1        default_CIFS      txt
vs1             default_CIFS      txt
vs1             policy1           mp4, wav
vs1             policy3           wmv
vs2             default_CIFS      txt
vs2             policy2           mp3
6 entries were displayed.
```

vserver vscan on-access-policy file-ext-to-include add

Add to the list of file extensions to include

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

Description

The `vserver vscan on-access-policy file-ext-to-include add` command adds a file extension or list of file extensions to include for virus scanning to the specified policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a file extension or a list of file extensions to include for virus scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a file extension or a list of file extensions to include for virus scanning.

`-file-ext-to-include <File extension>,…` - File Extensions to Scan

This parameter specifies the file extension or a list of file extensions to include for virus scanning.

Examples

The following example adds a list of file extensions to include for virus scanning to the specified on-access policy.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include add
-vserver vs1
            -policy-name policy1 -file-ext-to-include "mp*","tx*"

cluster1::> vserver vscan on-access-policy file-ext-to-include show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
    File Extensions to Scan: mp*, tx*, wav
```

vserver vscan on-access-policy file-ext-to-include remove

Remove from the list of file extensions to include

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

Description

The `vserver vscan on-access-policy file-ext-to-include remove` command removes a file extension or list of file extension that are included for virus scanning from the specified policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a file extension or list of file extensions that are included for virus scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a file extension or a list of file extensions that are included for virus scanning.

`-file-ext-to-include <File extension>,…` - File Extensions to Scan

This parameter specifies the file extension or a list of file extensions that you want to remove from the specified on-access policy.

Examples

The following example removes a list of file extensions from the specified on-access policy.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include remove
-vserver vs1
            -policy-name policy1 -file-ext-to-include "txt*,"wav"

cluster1::> vserver vscan on-access-policy file-ext-to-include show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
    File Extensions to Scan: mp*
```

vserver vscan on-access-policy file-ext-to-include show

Display list of file extensions to include

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

Description

The `vserver vscan on-access-policy file-ext-to-include show` command displays the list of file extensions to include for virus scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on access policies:

- Vserver name
- Policy name
- List of File-Extensions to Scan

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 policies for the specified Vserver.

[-policy-name <Policy name>] - Policy

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

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the policies that have the specified file extensions that are included for virus scanning.

Examples

The following example displays the list of file extensions that are included for virus scanning for all policies.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include show
Vserver         Policy Name       File-Ext Included
--------------- -----------------
----------------------------------------
cluster1        default_CIFS      *
vs1             default_CIFS      *
vs1             policy1           mp*
vs1             policy3           doc*, xl*
vs2             default_CIFS      *
vs2             policy2           d*, m*, t*
6 entries were displayed.
```

vserver vscan on-access-policy paths-to-exclude add

Add to the list of paths to exclude

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

Description

The `vserver vscan on-access-policy paths-to-exclude add` command adds a path or a list of paths that must be excluded from scanning to the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a path or a list of paths that must be excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a path or a list of paths that must be excluded from scanning.

`-paths-to-exclude <File path>,…` - Paths Not to Scan

This parameter specifies the path or list of paths that must be excluded from scanning.

Examples

The following example adds a list of paths that must be excluded from scanning to the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy paths-to-exclude add -vserver
vs1
            -policy-name policy1 -paths-to-exclude \test\test2,\test\test3

cluster1::> vserver vscan on-access-policy paths-to-exclude show -vserver
vs1
            -policy-name policy1
Vserver: vs1
                Policy: policy1
File-Paths Not to Scan: \test\test1, \test\test2, \test\test3
```

vserver vscan on-access-policy paths-to-exclude remove

Remove from the list of paths to exclude

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

Description

The `vserver vscan on-access-policy paths-to-exclude remove` command removes a path or a list of paths that are excluded from scanning from the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a path or list of paths that are excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a path or a list of paths that are excluded from scanning.

`-paths-to-exclude <File path>,…` - Paths Not to Scan

This parameter specifies the path or a list of paths that must be removed from the on-access policy.

Examples

The following example removes a list of paths that are excluded from scanning from the specified policy name:

```
cluster:> vserver vscan on-access-policy paths-to-exclude remove -vserver
vs1
          -policy-name policy1 -paths-to-exclude \test\test2,\test\test3

cluster1:> vserver vscan on-access-policy paths-to-exclude show -vserver
vs1
          -policy-name policy1
Vserver: vs1
                Policy: policy1
File-Paths Not to Scan: \test\test1
```

vserver vscan on-access-policy paths-to-exclude show

Display list of paths to exclude

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

Description

The `vserver vscan on-access-policy paths-to-exclude show` command displays the list of paths that are excluded from scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on-access policies:

- Vserver name
- Policy name
- List of Paths to exclude

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 policy names for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified policy name.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the policies that have the specified paths that are excluded from scanning.

Examples

The following example displays the list of paths that are excluded from scanning for all the policies:

```
cluster1::> vserver vscan on-access-policy paths-to-exclude  show
Vserver         Policy Name       Paths Excluded
--------------- -----------------
----------------------------------------
cluster1        default_CIFS      \test\test1
vs1             default_CIFS      \test\test1
vs1             policy1           \test\test2,\test\test3
vs1             policy3           \test\test4
vs2             default_CIFS      \test\test1
vs2             policy2           \test\test5
6 entries were displayed.
```

vserver vscan on-demand-task create

Create an On-Demand task

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

Description

The `vserver vscan on-demand-task create` command creates an On-Demand task. The On-Demand task consists of a set of attributes that are used for configuring the scope of scanning. It also specifies the cron schedule at which the task should run.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an On-Demand task.

`-task-name <text>` - Task Name

This parameter specifies the name of the On-Demand task that you want to create. An On-Demand task name can be up to 256 characters long.

`-scan-paths <text>,…` - List of Scan Paths

This parameter specifies a list of paths, separated by commas, for virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/".

`-report-directory <text>` - Report Directory Path

This parameter specifies a directory path where the On-Demand report file is created. Each run for a task creates a new file. The report directory path is given from the root of the Vserver using UNIX path delimiter "/".

`[-schedule <text>]` - Job Schedule

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule.

A Vserver can have only one scheduled task at a time.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file that will be considered for virus scanning. By default, it is *10GB* .

[-paths-to-exclude <text>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/". By default, no paths are excluded. The path can be in one of the following forms:

- */dir1/dir2/name* - This would match "/dir1/dir2/name" as well as "/dir1/dir2/name/…".
- */dir1/dir2/name/* - This would only match "/dir1/dir2/name/…".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "/vol/a b/" and "/vol/a,b/" to the `-paths-to-exclude` in the CLI, type *"/vol/a b/","/vol/a,b/"* at the command prompt.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. By default, no file extensions are excluded. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. By default it is *** , which means all the file extensions are considered for virus scanning except those that match one of the patterns provided in `-file-ext-to-exclude` list. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not. By default, it is true.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout

This parameter specifies the timeout value for a scan request. It is used to specify the time interval in which the node waits for a response from the Vscan server. Beyond this timeout period, the scan request is considered as failed. The value for this field must be between 10s and 1h. By default, it is 5m.

[-cross-junction {true|false}] - Cross Junction

This parameter specifies if the On-Demand task is allowed to cross volume junctions. If the parameter is set to false, crossing junctions is not allowed. By default, it is true.

[-directory-recursion {true|false}] - Directory Recursion

This parameter specifies if the On-Demand task is allowed to recursively scan through sub-directories. If the parameter is set to false, recursive scanning is not allowed. By default, it is true.

[-scan-priority {low|normal}] - Scan Priority

This parameter specifies the priority of the On-Demand scan requests generated by this task compared to On-Access scan requests. By default, it is low.

[-report-log-level {verbose|info|error}] - Report Log Level

This parameter specifies the log level of the On-Demand report. By default, it is info.

[-report-expiry-time <[<integer>h][<integer>m][<integer>s]>] - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example creates an On-Demand task:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name t1
            -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
            -schedule daily -max-file-size 5GB -paths-to-exclude
"/vol1/cold-files/"
            -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude
"mp3","mp4"
            -scan-files-with-no-ext false -request-timeout 2m -cross
-junction false
            -directory-recursion true -scan-priority low -report-log-level
verbose
            -report-expiry-time 12h
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 2m
                    Cross Junction: false
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task delete

Delete an On-Demand task

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

Description

The `vserver vscan on-demand-task delete` command deletes an On-Demand task.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver from which you want to delete an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to delete.

Examples

The following example deletes an On-Demand task:

```
cluster1::> vserver vscan on-demand-task delete -vserver vs1 -task-name t1

cluster1::> vserver vscan on-demand-task show -vserver vs1 -task-name t1
There are no entries matching your query.
```

vserver vscan on-demand-task modify

Modify an On-Demand task

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

Description

The `vserver vscan on-demand-task modify` command modifies an On-Demand task. The On-Demand task consists of a set of attributes that are used for configuring the scope of scanning. It also specifies the cron schedule at which the task should run.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to modify.

[-scan-paths <text>,…] - List of Scan Paths

This parameter specifies a list of paths, separated by commas, for virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/".

[-report-directory <text>] - Report Directory Path

This parameter specifies a directory path where the On-Demand report file is created. Each run for a task creates a new file. The report directory path is given from the root of the Vserver using UNIX path delimiter "/".

[-schedule <text>] - Job Schedule

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule. Providing empty schedule ("") unschedules the task.

A Vserver can have only one scheduled task at a time.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning.

[-paths-to-exclude <text>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/". The path can be in one of the following forms:

- */dir1/dir2/name* - This would match "/dir1/dir2/name" as well as "/dir1/dir2/name/…".
- */dir1/dir2/name/* - This would only match "/dir1/dir2/name/…".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "/vol/a b/" and "/vol/a,b/" to the `-paths-to-exclude` in the CLI, type *"/vol/a b/","/vol/a,b/"* at the command prompt.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout

This parameter specifies the timeout value for a scan request. It is used to specify the time interval in which the node waits for a response from the Vscan server. Beyond this timeout period, the scan request is considered as failed. The value for this field must be between 10s and 1h.

[-cross-junction {true|false}] - Cross Junction

This parameter specifies if the On-Demand task is allowed to cross volume junctions. If the parameter is set to false, crossing junctions is not allowed.

[-directory-recursion {true|false}] - Directory Recursion

This parameter specifies if the On-Demand task is allowed to recursively scan through sub-directories. If the parameter is set to false, recursive scanning is not allowed.

[-scan-priority {low|normal}] - Scan Priority

This parameter specifies the priority of the On-Demand scan requests generated by this task compared to On-Access scan requests.

[-report-log-level {verbose|info|error}] - Report Log Level

This parameter specifies the log level of the On-Demand report.

[-report-expiry-time <[<integer>h][<integer>m][<integer>s]>] - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example modifies an On-Demand task:

```
cluster1::> vserver vscan on-demand-task modify -vserver vs1 -task-name t1
            -scan-paths "/vol3/","/vol4/cifs/" -report-directory "/report-
dir"
            -schedule custom -max-file-size 2GB -paths-to-exclude
"/vol1/cold-files/"
            -file-ext-to-include "*" -file-ext-to-exclude "mp3","mp4"
            -scan-files-with-no-ext true -request-timeout 1m -cross
-junction true
[Job 136]: Vscan On-Demand job is queued. Use the "job show -id 136"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /vol3/, /vol4/cifs/
             Report Directory Path: /report-dir
                      Job Schedule: custom
Max File Size Allowed for Scanning: 2GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task run

Run an On-Demand task

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

Description

The `vserver vscan on-demand-task run` command start virus scanning immediately for an On-Demand task.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to start start virus scanning.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to start virus scanning.

Examples

The following example starts virus scanning an On-Demand task:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name t1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

vserver vscan on-demand-task schedule

Schedule an On-Demand task

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

Description

The `vserver vscan on-demand-task schedule` command schedules an On-Demand task.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to schedule an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to schedule.

-schedule <text> - Schedule Name

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule.

A Vserver can have only one scheduled task at a time.

Examples

The following example schedules an On-Demand task:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs1 -task-name
t1 -schedule daily
[Job 150]: Vscan On-Demand job is queued. Use the "job show -id 150"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /test
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 2GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: verbose
```

vserver vscan on-demand-task show

Display On-Demand tasks

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

Description

The `vserver vscan on-demand-task show` command displays information about the On-Demand tasks belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all On-Demand tasks:

- Vserver name
- Task name
- Scan paths
- Report directory path
- Schedule

You can specify the `-fields` parameter to specify which fields of information to display about On-Demand tasks. In addition to the fields above, you can display the following fields:

- Max file size
- File paths to exclude

- File extensions to exclude
- File extensions to include
- Scan files without extension
- Scan timeout
- Cross junction
- Directory recursion
- Scan priority
- Report log level

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 On-Demand tasks for the specified Vserver.

[-task-name <text>] - Task Name

If you specify this parameter, the command displays information only about the specified On-Demand task.

[-scan-paths <text>,…] - List of Scan Paths

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified path or paths in the scan-paths list.

[-report-directory <text>] - Report Directory Path

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified report-directory.

[-schedule <text>] - Job Schedule

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified schedule.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified max-file-size.

[-paths-to-exclude <text>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified path or paths in the exclude list.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified file extension or extensions in the exclude list.

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified file extension or extensions in the include list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified request-timeout.

[-cross-junction {true|false}] - Cross Junction

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-directory-recursion {true|false}] - Directory Recursion

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-scan-priority {low|normal}] - Scan Priority

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified scan-priority.

[-report-log-level {verbose|info|error}] - Report Log Level

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified report-log-level.

[-report-expiry-time <[<integer>h][<integer>m][<integer>s]>] - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example displays information about all On-Demand tasks:

```
cluster1::> vserver vscan on-demand-task show
                                          Report
Vserver     Task Name   Scan Paths          Directory Path    Schedule
----------- ----------  ------------------- -----------------
--------------
vs1         t1          /test               /report           -
vs2         t2          /, /test/           /report           daily
2 entries were displayed.
```

The following example displays detailed information about an On-Demand task:

```
cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                           Task Name: t1
                 List of Scan Paths: /test
              Report Directory Path: /report
                        Job Schedule: -
Max File Size Allowed for Scanning: 2GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: verbose
```

vserver vscan on-demand-task unschedule

Unschedule an On-Demand task

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

Description

The `vserver vscan on-demand-task unschedule` command unschedules an On-Demand task.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the name of the Vserver on which you want to unschedule an On-Demand task.

`-task-name <text>` - Task Name
This parameter specifies the name of the On-Demand task that you want to unschedule.

Examples

The following example unschedules an On-Demand task:

```
cluster1::> vserver vscan on-demand-task unschedule -vserver vs1 -task
-name t1

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /test
             Report Directory Path: /report
                       Job Schedule: -
Max File Size Allowed for Scanning: 2GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task report delete

Delete an On-Demand report

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

Description

The `vserver vscan on-demand-task report delete` command deletes an On-Demand report.

Parameters

`-vserver <vserver name>` - Vserver
This parameter specifies the name of the Vserver from which you want to delete an On-Demand report.

`-task-name <text>` - Task Name
This parameter specifies the name of the On-Demand task whose report you want to delete.

`-report-file <text>` - Report File Path
This parameter specifies the path of the report-file whose report record you want to delete.

`[-delete-report-file {true|false}]` - Delete Report File Also
This parameter specifies if the corresponding report file is also to be deleted. By default, it is false.

Examples

The following example deletes only On-Demand report record:

```
cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log

cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log
There are no entries matching your query.
```

The following example deletes an On-Demand report file along with the report record:

```
cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log -delete-report
-file true

cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log -delete-report
-file true
There are no entries matching your query.
```

vserver vscan on-demand-task report show

Display On-Demand reports

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

Description

The `vserver vscan on-demand-task report show` command displays information about the On-Demand reports belonging to the Vserver. A new report record is generated at the end of an On-Demand task run. If you do not specify any parameters, the command displays the following information about all On-Demand tasks:

- Vserver name
- Task name
- Report file path
- Number of clean files
- Number of infected files

You can specify the `-fields` parameter to specify which fields of information to display about On-Demand

report. In addition to the fields above, you can display the following fields:

- Job ID
- Job duration
- Number of attempted scans
- Number of files skipped from scanning
- Number of already scanned files
- Number of successful scans
- Number of failed scans
- Number of timed-out scans
- Job start time
- Job end time

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 On-Demand reports for the specified Vserver.

[-task-name <text>] - Task Name

If you specify this parameter, the command displays information only about the On-Demand reports for the specified task.

[-report-file <text>] - Report File Path

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified report file-path.

[-job-id <integer>] - Job ID

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified job ID.

[-job-duration <[<integer>h][<integer>m][<integer>s]>] - Job Duration

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-attempted-scans <integer>] - Number of Attempted Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-skipped-scans <integer>] - Number of Files Skipped from Scanning

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-already-scanned-files <integer>] - Number of Already Scanned Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-successful-scans <integer>] - Number of Successful Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-failed-scans <integer>] - Number of Failed Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-timedout-scans <integer>] - Number of Timedout Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-files-cleaned <integer>] - Number of Clean Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-files-infected <integer>] - Number of Infected Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-internal-error <integer>] - Number of Internal Error (privilege: advanced)

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-scan-retries <integer>] - Number of Scan Retries (privilege: advanced)

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-job-start-time <MM/DD/YYYY HH:MM:SS>] - Job Start Time

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-job-end-time <MM/DD/YYYY HH:MM:SS>] - Job End Time

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

Examples

The following example displays information about all On-Demand reports:

```
cluster1::> vscan on-demand-task report show
                                                                  Files
Files
Vserver     Task Name   Report File Path                     Cleaned
Infected
----------- ----------  ---------------------------------- ---------
---------
vs1         t1          /rep/avod_146_20150902_161439.log       6240
5
vs1         t1          /rep/avod_149_20150903_160313.log        115
0
2 entries were displayed.
```

The following example displays detailed information about an On-Demand task:

```
cluster1::> vscan on-demand-task report show -vserver vs1 -task-name t1
            -report-file /rep/avod_146_20150902_161439.log
Vserver: vs1
                            Task Name: t1
                     Report File Path: /rep/avod_146_20150902_161439.log
                               Job ID: 146
                         Job Duration: 76s
             Number of Attempted Scans: 6245
Number of Files Skipped from Scanning: 1286
      Number of Already Scanned Files: 987
           Number of Successful Scans: 6245
               Number of Failed Scans: 0
             Number of Timedout Scans: 0
                Number of Clean Files: 6240
             Number of Infected Files: 5
                       Job Start Time: 9/2/2015 16:14:39
                         Job End Time: 9/2/2015 16:15:55
```

vserver vscan scanner-pool apply-policy

Apply scanner-policy to a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool apply-policy` command applies a scanner policy to the specified scanner pool on a specified Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to apply the scanner policy. The Vserver administrator can apply the scanner policy to a scanner pool created within the scope of the Vserver or the cluster. The cluster administrator can apply the scanner policy to a scanner pool for any Vserver but cannot apply it within the scope of cluster. The scope is determined at a Vserver level.

-scanner-pool <Scanner pool> - Scanner Pool

This parameter specifies the name of the scanner pool.

-scanner-policy <Scanner policy> - Scanner Policy

This parameter specifies the scanner policy that you want to apply to the specified scanner pool on a Vserver. Currently only system policies are available. Available system policies are:

- *primary* - Makes it active always.
- *secondary* - Makes it active only when none of the primary external virus-scanning servers are connected.
- *idle* - Makes it inactive always.

[-cluster <Cluster name>] - Cluster on Which Policy Is Applied

This parameter specifies the name of the cluster on which you want to apply the scanner policy of a scanner pool. By default, it is applied on the local cluster. This parameter does not have any significance if the cluster is not in a DR relationship.

Examples

The following command applies a scanner policy to the specified scanner pool on a specified Vserver.

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
            -scanner-pool p1 -scanner-policy primary -cluster cluster2

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool p1
Vserver: vs1
                        Scanner Pool: p1
                      Applied Policy: primary
                      Current Status: on
  Cluster on Which Policy Is Applied: cluster2
           Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
            List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool create

Create a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool create` command creates a Vscan scanner pool. Scanner pool is a set of attributes which are used to validate and manage connection between clustered Data ONTAP and external virus-scanning server, or "Vscan server". It also specifies other parameters which are used for connection management. After creating a scanner pool, a scanner-policy must be applied to it using the command vserver vscan scanner-pool apply-policy . The default applied policy is *idle* , which means the scanner pool is inactive.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to create a scanner pool.

-scanner-pool <Scanner pool> - Scanner Pool

This parameter specifies the name of the scanner pool. Scanner pool 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 ".".

-hostnames <text>,... - List of Host Names of Allowed Vscan Servers

This parameter specifies a list of host names or IP addresses of the Vscan servers which are allowed to connect to clustered Data ONTAP.

-privileged-users <Privileged user>,... - List of Privileged Users

This parameter specifies a list of privileged users. A valid form of privileged user-name is "domain-name\user-name" and can be up to 256 characters long. Privileged user-names are stored and treated as case-insensitive strings. Virus scanners must use one of the registered privileged users for connecting to clustered Data ONTAP for exchanging virus-scanning protocol messages and to access file for scanning, remedying and quarantining operations.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request. It specifies the time interval in which the node waits for a response from the Vscan server. If the timeout is reached, the node allows the file-operation if the applicable On-Access policy has scan-mandatory set to 'off'. If the policy has scan-mandatory set to 'on', then the node will retry the scan or disallow the file-operation depending on the remaining lifetime of the CIFS request. Valid values for this field are from 10s to 40s. However, if scan-mandatory is set to 'off', the effective value is limited to a maximum of 35s. The default value is 30s.

[-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request in scan-engine's queue. The value for this field must be between 10s and 30s. By default, it is 20s.

[-session-setup-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-setup-message. The value for this field must be between 5s and 10s. By default, it is 10s.

[-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-teardown-message, or for any

message to be received for a session-id, after the underlying connection has been disconnected. The value for this field must be between 5s and 10s. By default, it is 10s.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

This parameter specifies the maximum number of consecutive session-setup attempts. The value for this field must be between 1 and 10. By default, it is 5.

Examples

The following example creates a scanner pool.

```
Cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP
            -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

Related Links

- vserver vscan scanner-pool apply-policy

vserver vscan scanner-pool delete

Delete a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool delete` command deletes a scanner pool.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete a scanner pool.

-scanner-pool <Scanner pool> - Scanner Pool

This parameter specifies the name of the scanner-pool that you want to delete.

Examples

The following example deletes a scanner pool.

```
cluster1::> vserver vscan scanner-pool delete -vserver vs1 -scanner-pool
test

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
test
There are no entries matching your query.
```

vserver vscan scanner-pool modify

Modify a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool modify` command modifies a Vscan scanner pool. Scanner pool is a set of attributes which are used to validate and manage connection between clustered Data ONTAP and external virus-scanning server, or "Vscan server". It also specifies other parameters which are used for connection management.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify a scanner pool.

-scanner-pool <Scanner pool> - Scanner Pool

This parameter specifies the name of the scanner pool. Scanner pool 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 ".".

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

This parameter specifies a list of host names or IP addresses of the Vscan servers which are allowed to connect to clustered Data ONTAP.

[-privileged-users <Privileged user>,…] - List of Privileged Users

This parameter specifies a list of privileged users. A valid form of privileged user-name is "domain-name\user-name" and can be up to 256 characters long. Privileged user-names are stored and treated as case-insensitive strings. Virus scanners must use one of the registered privileged users for connecting to clustered Data ONTAP for exchanging virus-scanning protocol messages and to access file for scanning, remedying and quarantining operations.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request. It specifies the time interval in which the node waits for a response from the Vscan server. If the timeout is reached, the node allows the file-operation if the applicable On-Access policy has scan-mandatory set to 'off'. If the policy has scan-mandatory set to 'on', then the node will retry the scan or disallow the file-operation depending on the remaining lifetime of the CIFS request. Valid values for this field are from 10s to 40s. However, if scan-mandatory is set to 'off', the effective value is limited to a maximum of 35s.

[-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request in scan-engine's queue. The value for this field must be between 10s and 30s.

[-session-setup-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-setup-message. The value for this field must be between 5s and 10s.

[-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-teardown-message, or for any message to be received for a session-id, after the underlying connection has been disconnected. The value for this field must be between 5s and 10s.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

This parameter specifies the maximum number of consecutive session-setup attempts. The value for this field must be between 1 and 10.

Examples

The following example modifies a scanner pool.

```
Cluster1::> vserver vscan scanner-pool modify -vserver vs1 -scanner-pool
SP
            -hostnames 2.2.2.2,vmwin204-29.fsct.nb -privileged-users
cifs\u3

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 2.2.2.2, 10.72.204.29
List of Host Names of Allowed Vscan Servers: 2.2.2.2, vmwin204-29.fsct.nb
                   List of Privileged Users: cifs\u3
```

vserver vscan scanner-pool resolve-hostnames

Resolve the hostnames configured in the scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool resolve-hostnames` command resolves the host names configured in the scanner pool and update it with the IP addressses. This command also updates the active scanner pool configuration of the Vserver if the scanner pool is part of that. You must run this command for the scanner pool whose host name entry is modified in the DNS server.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the name of the Vserver for which you want to resolve host names.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool for which you want to resolve host names.

Examples

The following example resolves the host names of a scanner pool:

```
cluster1::> vserver vscan scanner-pool resolve-hostnames -vserver vs1
-scanner-pool SP

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: Cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 10.72.204.27, 10.72.204.29
List of Host Names of Allowed Vscan Servers: vmwin204-27.fsct.nb,
vmwin204-29.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool show-active

Display active scanner pools

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool show-active` command displays active scanner pool information available to the Vserver. The active scanner pool configuration is derived by merging the information of the scanner pools which are currently active on a Vserver. If you do not specify any parameters, the command displays the following information about all Vservers:

- Vserver name
- List of scanner pools
- List of servers
- List of privileged user

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 specified Vserver.

[-scanner-pools <Scanner pool>,…] - List of Enabled Scanner Pools

If you specify this parameter, the command displays information only about the Vservers that have the specified scanner pool or pools. A scanner pool becomes part of this list if it is active at this time.

[-servers <IP Address>,…] - Merged List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the Vservers that have the specified server or servers. Servers of all active scanner pools on a Vserver are merged to derive this effective server list.

[-privileged-users <Privileged user>,…] - Merged List of Privileged Users

If you specify this parameter, the command displays information only about the Vservers that have the specified privileged user or users. Privileged users of all active scanner pools on a Vserver are merged to derive this effective privileged user list.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified request-timeout. This is set to the maximum value of the request-timeout of all active scanner pools on a Vserver.

[-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified scan-queue-timeout. This is set to the maximum value of the scan-queue-timeout of all active scanner pools on a Vserver.

[-session-setup-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified session-setup-timeout. This is set to the maximum value of the session-setup-timeout of all active scanner pools on a Vserver.

[-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified session-teardown-timeout. This is set to the maximum value of the session-teardown-timeout of all active scanner pools on a Vserver.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified max-session-setup-retries. This is set to the maximum number of the max-session-setup-retry of all active scanner pools on a Vserver.

Examples

The following example displays information about active scanner pool on all Vservers.

```
cluster1::> vserver vscan scanner-pool show
            Scanner    Pool                          Privileged
Scanner
Vserver     Pool       Owner   Servers               Users           Policy
----------- ---------- ------- -------------------- ---------------
----------
Cluster     clus       cluster 5.5.5.5              cifs\u5         idle
vs1         new        vserver 1.1.1.1, 2.2.2.2     cifs\u1
primary
vs1         clus       cluster 5.5.5.5              cifs\u5         idle
vs1         p1         vserver 3.3.3.3              cifs\u4
primary
vs2         clus       cluster 5.5.5.5              cifs\u5
primary
vs2         p2         vserver 3.3.3.3, 4.4.4.4     cifs\u2
primary
6 entries were displayed.

cluster1::> vserver vscan scanner-pool show-active
                                                      Privileged
Vserver     Scanner Pools      Servers                     Users
----------- ------------ --------------------------
------------------------
vs1         new, p1       1.1.1.1, 2.2.2.2, 3.3.3.3   cifs\u1, cifs\u4
vs2         clus, p2      3.3.3.3, 4.4.4.4, 5.5.5.5   cifs\u2, cifs\u5
2 entries were displayed.
```

vserver vscan scanner-pool show

Display scanner pools

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool show` command displays information about the Vscan scanner pools belonging to the Vserver. It also displays the scanner policy applied to the scanner pool and its current status in Vserver scope. If you do not specify any parameters, the command displays the following information about all scanner pools:

- Vserver name
- Scanner pool
- Scanner pool owner
- Scanner policy
- Current status

- Cluster on which policy is applied
- List of servers
- List of host names
- List of privileged user

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 scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only about the specified scanner pool.

[-scanner-policy <Scanner policy>] - Applied Policy

If you specify this parameter, the command displays information only about the scanner pools for the specified scanner policy.

[-current-status {on|off}] - Current Status

If you specify this parameter, the command displays information only about the scanner pools that have the specified status.

[-cluster <Cluster name>] - Cluster on Which Policy Is Applied

If you specify this parameter, the command displays information only about the scanner pools that are applied to the specified cluster.

[-owner <Configuration owner>] - Scanner Pool Config Owner

If you specify this parameter, the command displays information only about the scanner pools that have the specified owner.

[-servers <IP Address>,…] - List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified IP address or IP addresses.

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified host name or host names.

[-privileged-users <Privileged user>,…] - List of Privileged Users

If you specify this parameter, the command displays information only about the scanner pools that have the specified privileged user or users.

[-request-timeout <[<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified request-timeout.

[-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified scan-queue-timeout.

[-session-setup-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified session-setup-timeout.

[-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified session-teardown-timeout.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified max-session-setup-retries.

Examples

The following example displays information about all scanner pools.

```
Cluster1::> vserver vscan scanner-pool show
            Scanner    Pool                          Privileged
Scanner
Vserver     Pool       Owner   Servers               Users           Policy
----------- ---------- ------- --------------------- ---------------
----------
vs1         SP         vserver 1.1.1.1,              cifs\u1,
primary
                               10.72.204.27          cifs\u2
vs1         p1         vserver 3.3.3.3               cifs\u1,
secondary
                                                     cifs\u2
2 entries were displayed.
```

The following example displays detailed information about one scanner pool.

```
Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: Cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool privileged-users add

Add to the list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users add` command adds one privileged users or list of privileged users to the specified scanner pool.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to add a privileged user or users.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool to which you want to add a privileged user or users.

`-privileged-users <Privileged user>,…` - List of Privileged Users

This parameter specifies the privileged user or users that you want to add to the specified scanner pool.

Examples

The following example adds a list of privileged users to the specified scanner pool.

```
cluster1::> vserver vscan scanner-pool privileged-users add -vserver vs1
            -scanner-pool p1 -privileged-users cifs\u2,cifs\u3

cluster1::> vserver vscan scanner-pool privileged-users show -vserver vs1
            -scanner-pool p1
Vserver: vs1
            Scanner Pool: p1
List of Privileged Users: cifs\u1, cifs\u2, cifs\u3
```

vserver vscan scanner-pool privileged-users remove

Remove from the list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users remove` command removes one privileged users or list of privileged users from the specified scanner pool. All the existing privileged users of a scanner pool cannot be removed.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to remove a privileged user or users.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool from which you want to remove a privileged user or users.

`-privileged-users <Privileged user>,…` - List of Privileged Users

This parameter specifies the privileged user or users that you want to remove from the specified scanner pool.

Examples

The following example removes a list of privileged users from the specified scanner pool.

```
cluster1::> vserver vscan scanner-pool privileged-users remove -vserver
vs1
            -scanner-pool p1 -privileged-users cifs\u2,cifs\u3

cluster1::> vserver vscan scanner-pool privileged-users show -vserver vs1
            -scanner-pool p1
Vserver: vs1
            Scanner Pool: p1
List of Privileged Users: cifs\u1
```

vserver vscan scanner-pool privileged-users show

Display list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users show` command displays the list of privileged

users of the Vscan scanner pools belonging to the Vserver. If you do not specify any parameters, the command displays the following information about the scanner pools:

- Vserver name
- Scanner pool
- List of privileged 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 you specify this parameter, the command displays information only about the scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only for the specified scanner pool.

[-privileged-users <Privileged user>,…] - List of Privileged Users

If you specify this parameter, the command displays information only about the scanner pools that have the specified privileged user or users.

Examples

The following example displays the list of privileged users of all scanner pools.

```
cluster1::> vserver vscan scanner-pool privileged-users show
Vserver         Scanner Pool      Privileged Users
--------------- -----------------
-------------------------------------------
Cluster         clus              cifs\u5
vs1             new               cifs\u7
vs1             clus              cifs\u5
vs1             p1                cifs\u1, cifs\u2
vs2             clus              cifs\u5
vs2             p2                cifs\u2
6 entries were displayed.
```

vserver vscan scanner-pool servers add

Add to the list of hostnames

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers add` command adds one server or list of servers to the specified scanner pool.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to add a server or servers.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool to which you want to add a server or servers.

`-hostnames <text>,…` - List of Host Names for Vscan Servers

This parameter specifies the host name or host names that you want to add to the specified scanner pool.

Examples

The following example adds a list of servers to the specified scanner pool.

```
Cluster1::> vserver vscan scanner-pool servers add -vserver vs1
            -scanner-pool SP -hostnames 2.2.2.2, vmwin204-27.fsct.nb

Cluster1::> vserver vscan scanner-pool servers show -vserver vs1 -scanner
-pool SP
Vserver: vs1
                               Scanner Pool: SP
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2,
10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2,
                                             vmwin204-27.fsct.nb
```

vserver vscan scanner-pool servers remove

Remove from the list of hostnames

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers remove` command removes one server or list of servers from the specified scanner pool. All the existing servers of a scanner pool cannot be removed.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to remove a server or servers.

-scanner-pool <Scanner pool> - Scanner Pool

This parameter specifies the name of the scanner pool from which you want to remove a server or servers.

-hostnames <text>,… - List of hostnames for Vscan Servers

This parameter specifies the host name or host names that you want to remove from the specified scanner pool.

Examples

The following example removes a list of servers from the specified scanner pool.

```
Cluster1::> vserver vscan scanner-pool servers remove -vserver vs1
-scanner-pool SP -hostnames vmwin204-27.fsct.nb

Cluster1::> vserver vscan scanner-pool servers show -vserver vs1 -scanner
-pool SP
Vserver: vs1
                                Scanner Pool: SP
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
 List of Host Names of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
```

vserver vscan scanner-pool servers show

Display list of servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers show` command displays the list of servers of the Vscan scanner pools belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all scanner pools:

- Vserver name
- Scanner pool
- List of servers

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 scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only for the specified scanner pool.

[-servers <IP Address>,…] - List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified IP address or IP addresses.

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified host name or host names.

Examples

The following example displays the list of servers of all scanner pools.

```
cluster1::> vserver vscan scanner-pool servers show
Vserver         Scanner Pool      Servers
--------------- -----------------
-----------------------------------------
vs1             SP                1.1.1.1, 10.72.204.27
vs2             p1                10.72.204.29
6 entries were displayed.
```

The following example displays the list of servers and host names of all scanner pools.

```
cluster1::> vserver vscan scanner-pool servers show -instance
Vserver: vs1
                              Scanner Pool: SP
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
Vserver: vs2
                              Scanner Pool: p1
       List of IPs of Allowed Vscan Servers: 10.72.204.29
List of Host Names of Allowed Vscan Servers: vmwin204-29.fsct.nb
2 entries were displayed.
```

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.