

# Veritas NetBackup™ Status Codes Reference Guide

UNIX, Windows, and Linux

Release 8.1.1



# Veritas NetBackup™ Status Codes Reference Guide

Last updated: 2018-02-16

Document version: NetBackup 8.1.1

## Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC  
500 E Middlefield Road  
Mountain View, CA 94043

<http://www.veritas.com>

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	NetBackup status codes .....	45
	NetBackup status codes .....	45
	NetBackup status code: 0 .....	45
	NetBackup status code: 1 .....	46
	NetBackup status code: 2 .....	50
	NetBackup status code: 3 .....	51
	NetBackup status code: 4 .....	52
	NetBackup status code: 5 .....	52
	NetBackup status code: 6 .....	53
	NetBackup status code: 7 .....	55
	NetBackup status code: 8 .....	55
	NetBackup status code: 9 .....	55
	NetBackup status code: 10 .....	56
	NetBackup status code: 11 .....	56
	NetBackup status code: 12 .....	58
	NetBackup status code: 13 .....	59
	NetBackup status code: 14 .....	63
	NetBackup status code: 15 .....	64
	NetBackup status code: 16 .....	64
	NetBackup status code: 17 .....	64
	NetBackup status code: 18 .....	64
	NetBackup status code: 19 .....	65
	NetBackup status code: 20 .....	65
	NetBackup status code: 21 .....	68
	NetBackup status code: 22 .....	69
	NetBackup status code: 23 .....	69
	NetBackup status code: 24 .....	70
	NetBackup status code: 25 .....	71
	NetBackup status code: 26 .....	74
	NetBackup status code: 27 .....	74
	NetBackup status code: 28 .....	75
	NetBackup status code: 29 .....	75
	NetBackup status code: 30 .....	76
	NetBackup status code: 31 .....	76
	NetBackup status code: 32 .....	76
	NetBackup status code: 33 .....	76

NetBackup status code: 34 .....	77
NetBackup status code: 35 .....	77
NetBackup status code: 36 .....	78
NetBackup status code: 37 .....	78
NetBackup status code: 38 .....	79
NetBackup status code: 39 .....	79
NetBackup status code: 40 .....	79
NetBackup status code: 41 .....	80
NetBackup status code: 42 .....	84
NetBackup status code: 43 .....	84
NetBackup status code: 44 .....	85
NetBackup status code: 45 .....	85
NetBackup status code: 46 .....	86
NetBackup status code: 47 .....	87
NetBackup status code: 48 .....	87
NetBackup status code: 49 .....	88
NetBackup status code: 50 .....	89
NetBackup status code: 51 .....	90
NetBackup status code: 52 .....	90
NetBackup status code: 53 .....	91
NetBackup status code: 54 .....	92
NetBackup status code: 55 .....	92
NetBackup status code: 56 .....	93
NetBackup status code: 57 .....	93
NetBackup status code: 58 .....	94
NetBackup status code: 59 .....	94
NetBackup status code: 60 .....	96
NetBackup status code: 61 .....	97
NetBackup status code: 63 .....	97
NetBackup status code: 64 .....	97
NetBackup status code: 65 .....	98
NetBackup status code: 66 .....	98
NetBackup status code: 67 .....	99
NetBackup status code: 68 .....	100
NetBackup status code: 69 .....	100
NetBackup status code: 70 .....	101
NetBackup status code: 71 .....	101
NetBackup status code: 72 .....	102
NetBackup status code: 73 .....	102
NetBackup status code: 74 .....	102
NetBackup status code: 75 .....	103
NetBackup status code: 76 .....	103
NetBackup status code: 77 .....	103

NetBackup status code: 78 .....	104
NetBackup status code: 79 .....	105
NetBackup status code: 80 .....	105
NetBackup status code: 81 .....	105
NetBackup status code: 82 .....	106
NetBackup status code: 83 .....	106
NetBackup status code: 84 .....	108
NetBackup status code: 85 .....	109
NetBackup status code: 86 .....	110
NetBackup status code: 87 .....	111
NetBackup status code: 89 .....	111
NetBackup status code: 90 .....	113
NetBackup status code: 91 .....	114
NetBackup status code: 92 .....	114
NetBackup status code: 93 .....	115
NetBackup status code: 94 .....	116
NetBackup status code: 95 .....	116
NetBackup status code: 96 .....	117
NetBackup status code: 97 .....	119
NetBackup status code: 98 .....	119
NetBackup status code: 99 .....	119
NetBackup status code: 100 .....	120
NetBackup status code: 101 .....	121
NetBackup status code: 102 .....	121
NetBackup status code: 103 .....	121
NetBackup status code: 104 .....	122
NetBackup status code: 105 .....	122
NetBackup status code: 106 .....	122
NetBackup status code: 108 .....	123
NetBackup status code: 109 .....	123
NetBackup status code: 110 .....	124
NetBackup status code: 111 .....	124
NetBackup status code: 112 .....	125
NetBackup status code: 114 .....	125
NetBackup status code: 116 .....	125
NetBackup status code: 117 .....	126
NetBackup status code: 118 .....	128
NetBackup status code: 120 .....	130
NetBackup status code: 121 .....	130
NetBackup status code: 122 .....	130
NetBackup status code: 123 .....	131
NetBackup status code: 124 .....	131
NetBackup status code: 125 .....	131

NetBackup status code: 126 .....	132
NetBackup status code: 127 .....	132
NetBackup status code: 128 .....	132
NetBackup status code: 129 .....	133
NetBackup status code: 130 .....	134
NetBackup status code: 131 .....	134
NetBackup status code: 132 .....	135
NetBackup status code: 133 .....	135
NetBackup status code: 134 .....	136
NetBackup status code: 135 .....	137
NetBackup status code: 136 .....	137
NetBackup status code: 140 .....	138
NetBackup status code: 141 .....	138
NetBackup status code: 142 .....	138
NetBackup status code: 143 .....	139
NetBackup status code: 144 .....	139
NetBackup status code: 145 .....	140
NetBackup status code: 146 .....	140
NetBackup status code: 147 .....	141
NetBackup status code: 148 .....	141
NetBackup status code: 149 .....	141
NetBackup status code: 150 .....	142
NetBackup status code: 152 .....	142
NetBackup status code: 153 .....	142
NetBackup status code: 154 .....	142
NetBackup status code: 155 .....	143
NetBackup status code: 156 .....	143
NetBackup status code: 157 .....	157
NetBackup status code: 158 .....	157
NetBackup status code: 159 .....	157
NetBackup status code: 160 .....	158
NetBackup status code: 161 .....	159
NetBackup status code: 162 .....	159
NetBackup status code: 163 .....	159
NetBackup status code: 164 .....	159
NetBackup status code: 165 .....	160
NetBackup status code: 166 .....	160
NetBackup status code: 167 .....	160
NetBackup status code: 168 .....	161
NetBackup status code: 169 .....	161
NetBackup status code: 170 .....	161
NetBackup status code: 171 .....	163
NetBackup status code: 172 .....	163

NetBackup status code: 173 .....	164
NetBackup status code: 174 .....	164
NetBackup status code: 175 .....	166
NetBackup status code: 176 .....	166
NetBackup status code: 177 .....	167
NetBackup status code: 178 .....	167
NetBackup status code: 179 .....	168
NetBackup status code: 180 .....	168
NetBackup status code: 181 .....	168
NetBackup status code: 182 .....	169
NetBackup status code: 183 .....	169
NetBackup status code: 184 .....	170
NetBackup status code: 185 .....	171
NetBackup status code: 186 .....	171
NetBackup status code: 189 .....	172
NetBackup status code: 190 .....	172
NetBackup status code: 191 .....	172
NetBackup status code: 192 .....	174
NetBackup status code: 193 .....	175
NetBackup status code: 194 .....	175
NetBackup status code: 195 .....	175
NetBackup status code: 196 .....	176
NetBackup status code: 197 .....	176
NetBackup status code: 198 .....	177
NetBackup status code: 199 .....	177
NetBackup status code: 200 .....	178
NetBackup status code: 201 .....	178
NetBackup status code: 202 .....	179
NetBackup status code: 203 .....	181
NetBackup status code: 204 .....	181
NetBackup status code: 205 .....	183
NetBackup status code: 206 .....	184
NetBackup status code: 207 .....	185
NetBackup status code: 209 .....	186
NetBackup status code: 210 .....	186
NetBackup status code: 212 .....	186
NetBackup status code: 213 .....	187
NetBackup status code: 215 .....	188
NetBackup status code: 216 .....	188
NetBackup status code: 217 .....	189
NetBackup status code: 218 .....	189
NetBackup status code: 219 .....	190
NetBackup status code: 220 .....	191



NetBackup status code: 221 .....	191
NetBackup status code: 222 .....	192
NetBackup status code: 223 .....	192
NetBackup status code: 224 .....	192
NetBackup status code: 225 .....	193
NetBackup status code: 226 .....	193
NetBackup status code: 227 .....	193
NetBackup status code: 228 .....	194
NetBackup status code: 229 .....	194
NetBackup status code: 230 .....	194
NetBackup status code: 231 .....	195
NetBackup status code: 232 .....	195
NetBackup status code: 233 .....	195
NetBackup status code: 234 .....	196
NetBackup status code: 235 .....	196
NetBackup status code: 236 .....	196
NetBackup status code: 237 .....	197
NetBackup status code: 238 .....	197
NetBackup status code: 239 .....	197
NetBackup status code: 240 .....	197
NetBackup status code: 241 .....	198
NetBackup status code: 242 .....	198
NetBackup status code: 243 .....	198
NetBackup status code: 245 .....	199
NetBackup status code: 246 .....	199
NetBackup status code: 247 .....	199
NetBackup status code: 248 .....	199
NetBackup status code: 249 .....	200
NetBackup status code: 250 .....	200
NetBackup status code: 251 .....	200
NetBackup status code: 252 .....	201
NetBackup status code: 253 .....	201
NetBackup status code: 254 .....	201
NetBackup status code: 256 .....	201
NetBackup status code: 257 .....	202
NetBackup status code: 258 .....	202
NetBackup status code: 259 .....	202
NetBackup status code: 260 .....	202
NetBackup status code: 261 .....	203
NetBackup status code: 262 .....	203
NetBackup status code: 263 .....	203
NetBackup status code: 265 .....	203
NetBackup status code: 266 .....	204

NetBackup status code: 267 .....	204
NetBackup status code: 268 .....	205
NetBackup status code: 269 .....	205
NetBackup status code: 270 .....	205
NetBackup status code: 271 .....	206
NetBackup status code: 272 .....	206
NetBackup status code: 273 .....	206
NetBackup status code: 274 .....	207
NetBackup status code: 275 .....	207
NetBackup status code: 276 .....	207
NetBackup status code: 277 .....	207
NetBackup status code: 278 .....	208
NetBackup status code: 279 .....	208
NetBackup status code: 280 .....	208
NetBackup status code: 281 .....	208
NetBackup status code: 282 .....	209
NetBackup status code: 283 .....	209
NetBackup status code: 284 .....	209
NetBackup status code: 285 .....	210
NetBackup status code: 286 .....	210
NetBackup status code: 287 .....	210
NetBackup status code: 288 .....	211
NetBackup status code: 289 .....	211
NetBackup status code: 290 .....	211
NetBackup status code: 291 .....	212
NetBackup status code: 292 .....	212
NetBackup status code: 293 .....	213
NetBackup status code: 294 .....	214
NetBackup status code: 295 .....	215
NetBackup status code: 296 .....	215
NetBackup status code: 297 .....	215
NetBackup status code: 298 .....	216
NetBackup status code: 299 .....	216
NetBackup status code: 300 .....	217
NetBackup status code: 301 .....	217
NetBackup status code: 302 .....	218
NetBackup status code: 303 .....	219
NetBackup status code: 304 .....	219
NetBackup status code: 305 .....	219
NetBackup status code: 306 .....	220
NetBackup status code: 307 .....	220
NetBackup status code: 308 .....	220
NetBackup status code: 309 .....	221

NetBackup status code: 310 .....	221
NetBackup status code: 311 .....	222
NetBackup status code: 312 .....	222
NetBackup status code: 313 .....	222
NetBackup status code: 314 .....	223
NetBackup status code: 315 .....	223
NetBackup status code: 316 .....	223
NetBackup status code: 317 .....	224
NetBackup status code: 318 .....	224
NetBackup status code: 319 .....	224
NetBackup status code: 320 .....	225
NetBackup status code: 321 .....	225
NetBackup status code: 322 .....	225
NetBackup status code: 323 .....	226
NetBackup status code: 324 .....	226
NetBackup status code: 325 .....	227
NetBackup status code: 326 .....	227
NetBackup status code: 327 .....	227
NetBackup status code: 328 .....	228
NetBackup status code: 329 .....	228
NetBackup status code: 330 .....	228
NetBackup status code: 331 .....	229
NetBackup status code: 332 .....	229
NetBackup status code: 333 .....	229
NetBackup status code: 334 .....	230
NetBackup status code: 335 .....	230
NetBackup status code: 336 .....	230
NetBackup status code: 337 .....	230
NetBackup status code: 338 .....	231
NetBackup status code: 339 .....	231
NetBackup status code: 340 .....	231
NetBackup status code: 341 .....	231
NetBackup status code: 342 .....	232
NetBackup status code: 343 .....	232
NetBackup status code: 344 .....	232
NetBackup status code: 345 .....	233
NetBackup status code: 346 .....	233
NetBackup status code: 347 .....	233
NetBackup status code: 348 .....	233
NetBackup status code: 349 .....	234
NetBackup status code: 350 .....	234
NetBackup status code: 351 .....	234
NetBackup status code: 400 .....	235

NetBackup status code: 401 .....	235
NetBackup status code: 402 .....	235
NetBackup status code: 403 .....	236
NetBackup status code: 404 .....	236
NetBackup status code: 405 .....	237
NetBackup status code: 406 .....	237
NetBackup status code: 407 .....	238
NetBackup status code: 408 .....	238
NetBackup status code: 409 .....	238
NetBackup status code: 501 .....	239
NetBackup status code: 502 .....	239
NetBackup status code: 503 .....	239
NetBackup status code: 504 .....	240
NetBackup status code: 505 .....	240
NetBackup status code: 506 .....	241
NetBackup status code: 507 .....	242
NetBackup status code: 508 .....	242
NetBackup status code: 509 .....	243
NetBackup status code: 510 .....	243
NetBackup status code: 511 .....	244
NetBackup status code: 512 .....	244
NetBackup status code: 513 .....	245
NetBackup status code: 514 .....	245
NetBackup status code: 516 .....	246
NetBackup status code: 517 .....	246
NetBackup status code: 518 .....	247
NetBackup status code: 519 .....	247
NetBackup status code: 520 .....	248
NetBackup status code: 521 .....	248
NetBackup status code: 522 .....	248
NetBackup status code: 523 .....	248
NetBackup status code: 525 .....	249
NetBackup status code: 526 .....	250
NetBackup status code: 527 .....	250
NetBackup status code: 537 .....	250
NetBackup status code: 538 .....	251
NetBackup status code: 552 .....	251
NetBackup status code: 600 .....	252
NetBackup status code: 601 .....	252
NetBackup status code: 602 .....	252
NetBackup status code: 603 .....	253
NetBackup status code: 604 .....	253
NetBackup status code: 605 .....	253

NetBackup status code: 606 .....	254
NetBackup status code: 607 .....	254
NetBackup status code: 608 .....	255
NetBackup status code: 609 .....	255
NetBackup status code: 610 .....	255
NetBackup status code: 611 .....	256
NetBackup status code: 612 .....	256
NetBackup status code: 613 .....	257
NetBackup status code: 614 .....	257
NetBackup status code: 615 .....	258
NetBackup status code: 616 .....	258
NetBackup status code: 617 .....	258
NetBackup status code: 618 .....	258
NetBackup status code: 619 .....	259
NetBackup status code: 620 .....	259
NetBackup status code: 621 .....	259
NetBackup status code: 622 .....	260
NetBackup status code: 623 .....	260
NetBackup status code: 624 .....	260
NetBackup status code: 625 .....	261
NetBackup status code: 626 .....	261
NetBackup status code: 627 .....	262
NetBackup status code: 628 .....	262
NetBackup status code: 629 .....	262
NetBackup status code: 630 .....	263
NetBackup status code: 631 .....	263
NetBackup status code: 632 .....	263
NetBackup status code: 633 .....	264
NetBackup status code: 634 .....	264
NetBackup status code: 635 .....	265
NetBackup status code: 636 .....	265
NetBackup status code: 637 .....	265
NetBackup status code: 638 .....	266
NetBackup status code: 639 .....	266
NetBackup status code: 640 .....	267
NetBackup status code: 641 .....	267
NetBackup status code: 642 .....	268
NetBackup status code: 643 .....	268
NetBackup status code: 644 .....	268
NetBackup status code: 645 .....	269
NetBackup status code: 646 .....	270
NetBackup status code: 647 .....	270
NetBackup status code: 648 .....	270

NetBackup status code: 649 .....	271
NetBackup status code: 650 .....	271
NetBackup status code: 651 .....	272
NetBackup status code: 652 .....	272
NetBackup status code: 653 .....	272
NetBackup status code: 654 .....	273
NetBackup status code: 655 .....	273
NetBackup status code: 656 .....	273
NetBackup status code: 657 .....	274
NetBackup status code: 658 .....	274
NetBackup status code: 659 .....	275
NetBackup status code: 660 .....	275
NetBackup status code: 661 .....	275
NetBackup status code: 662 .....	276
NetBackup status code: 663 .....	276
NetBackup status code: 664 .....	277
NetBackup status code: 665 .....	277
NetBackup status code: 667 .....	277
NetBackup status code: 668 .....	278
NetBackup status code: 669 .....	278
NetBackup status code: 670 .....	278
NetBackup status code: 671 .....	279
NetBackup status code: 800 .....	279
NetBackup status code: 801 .....	279
NetBackup status code: 802 .....	280
NetBackup status code: 803 .....	281
NetBackup status code: 805 .....	281
NetBackup status code: 806 .....	282
NetBackup status code: 807 .....	283
NetBackup status code: 811 .....	283
NetBackup status code: 812 .....	283
NetBackup status code: 813 .....	283
NetBackup status code: 818 .....	284
NetBackup status code: 819 .....	284
NetBackup status code: 823 .....	284
NetBackup status code: 830 .....	285
NetBackup status code: 831 .....	285
NetBackup status code: 832 .....	286
NetBackup status code: 833 .....	286
NetBackup status code: 900 .....	287
NetBackup status code: 901 .....	287
NetBackup status code: 902 .....	287
NetBackup status code: 903 .....	288

NetBackup status code: 904 .....	288
NetBackup status code: 905 .....	289
NetBackup status code: 906 .....	289
NetBackup status code: 907 .....	289
NetBackup status code: 908 .....	290
NetBackup status code: 912 .....	290
NetBackup status code: 914 .....	291
NetBackup status code: 915 .....	291
NetBackup status code: 916 .....	291
NetBackup status code: 917 .....	292
NetBackup status code: 918 .....	292
NetBackup status code: 1000 .....	292
NetBackup status code: 1001 .....	293
NetBackup status code: 1002 .....	293
NetBackup status code: 1057 .....	293
NetBackup status code: 1058 .....	294
NetBackup status code: 1401 .....	294
NetBackup status code: 1402 .....	294
NetBackup status code: 1403 .....	295
NetBackup status code: 1405 .....	295
NetBackup status code: 1407 .....	295
NetBackup status code: 1408 .....	295
NetBackup status code: 1409 .....	295
NetBackup status code: 1410 .....	296
NetBackup status code: 1411 .....	296
NetBackup status code: 1412 .....	296
NetBackup status code: 1413 .....	296
NetBackup status code: 1414 .....	297
NetBackup status code: 1415 .....	297
NetBackup status code: 1416 .....	297
NetBackup status code: 1417 .....	297
NetBackup status code: 1418 .....	298
NetBackup status code: 1419 .....	298
NetBackup status code: 1420 .....	298
NetBackup status code: 1421 .....	298
NetBackup status code: 1422 .....	298
NetBackup status code: 1423 .....	299
NetBackup status code: 1425 .....	299
NetBackup status code: 1426 .....	299
NetBackup status code: 1500 .....	299
NetBackup status code: 1501 .....	300
NetBackup status code: 1502 .....	300
NetBackup status code: 1503 .....	301

NetBackup status code: 1504 .....	301
NetBackup status code: 1505 .....	302
NetBackup status code: 1506 .....	302
NetBackup status code: 1507 .....	302
NetBackup status code: 1508 .....	303
NetBackup status code: 1509 .....	303
NetBackup status code: 1510 .....	303
NetBackup status code: 1511 .....	304
NetBackup status code: 1512 .....	304
NetBackup status code: 1513 .....	304
NetBackup status code: 1514 .....	305
NetBackup status code: 1515 .....	305
NetBackup status code: 1516 .....	305
NetBackup status code: 1517 .....	306
NetBackup status code: 1518 .....	306
NetBackup status code: 1519 .....	306
NetBackup status code: 1521 .....	307
NetBackup status code: 1522 .....	307
NetBackup status code: 1523 .....	307
NetBackup status code: 1524 .....	307
NetBackup status code: 1525 .....	308
NetBackup status code: 1526 .....	308
NetBackup status code: 1527 .....	308
NetBackup status code: 1528 .....	309
NetBackup status code: 1529 .....	309
NetBackup status code: 1530 .....	310
NetBackup status code: 1531 .....	311
NetBackup status code: 1532 .....	311
NetBackup status code: 1533 .....	312
NetBackup status code: 1534 .....	312
NetBackup status code: 1535 .....	312
NetBackup status code: 1536 .....	313
NetBackup status code: 1537 .....	313
NetBackup status code: 1538 .....	314
NetBackup status code: 1539 .....	314
NetBackup status code: 1540 .....	315
NetBackup status code: 1541 .....	315
NetBackup status code: 1542 .....	315
NetBackup status code: 1543 .....	316
NetBackup status code: 1545 .....	316
NetBackup status code: 1546 .....	316
NetBackup status code: 1547 .....	316
NetBackup status code: 1548 .....	317



NetBackup status code: 1549 .....	317
NetBackup status code: 1552 .....	318
NetBackup status code: 1553 .....	318
NetBackup status code: 1554 .....	319
NetBackup status code: 1556 .....	319
NetBackup status code: 1557 .....	319
NetBackup status code: 1558 .....	320
NetBackup status code: 1559 .....	320
NetBackup status code: 1560 .....	320
NetBackup status code: 1561 .....	321
NetBackup status code: 1562 .....	321
NetBackup status code: 1563 .....	321
NetBackup status code: 1564 .....	322
NetBackup status code: 1565 .....	322
NetBackup status code: 1566 .....	322
NetBackup status code: 1567 .....	322
NetBackup status code: 1568 .....	323
NetBackup status code: 1569 .....	323
NetBackup status code: 1570 .....	323
NetBackup status code: 1571 .....	324
NetBackup status code: 1572 .....	324
NetBackup status code: 1573 .....	324
NetBackup status code: 1574 .....	325
NetBackup status code: 1575 .....	325
NetBackup status code: 1576 .....	325
NetBackup status code: 1577 .....	326
NetBackup status code: 1578 .....	326
NetBackup status code: 1579 .....	326
NetBackup status code: 1580 .....	326
NetBackup status code: 1581 .....	327
NetBackup status code: 1582 .....	327
NetBackup status code: 1583 .....	327
NetBackup status code: 1584 .....	328
NetBackup status code: 1585 .....	328
NetBackup status code: 1586 .....	328
NetBackup status code: 1587 .....	329
NetBackup status code: 1588 .....	329
NetBackup status code: 1589 .....	329
NetBackup status code: 1590 .....	329
NetBackup status code: 1591 .....	330
NetBackup status code: 1592 .....	330
NetBackup status code: 1593 .....	330
NetBackup status code: 1594 .....	331

NetBackup status code: 1596 .....	331
NetBackup status code: 1597 .....	331
NetBackup status code: 1598 .....	331
NetBackup status code: 1599 .....	332
NetBackup status code: 1600 .....	332
NetBackup status code: 1601 .....	332
NetBackup status code: 1602 .....	333
NetBackup status code: 1603 .....	333
NetBackup status code: 1604 .....	333
NetBackup status code: 1800 .....	334
NetBackup status code: 1915 .....	334
NetBackup status code: 1916 .....	334
NetBackup status code: 1917 .....	335
NetBackup status code: 1918 .....	335
NetBackup status code: 1919 .....	335
NetBackup status code: 1920 .....	336
NetBackup status code: 1921 .....	336
NetBackup status code: 1922 .....	336
NetBackup status code: 1924 .....	337
NetBackup status code: 1925 .....	337
NetBackup status code: 1926 .....	337
NetBackup status code: 1927 .....	338
NetBackup status code: 1928 .....	338
NetBackup status code: 2000 .....	338
NetBackup status code: 2001 .....	339
NetBackup status code: 2002 .....	340
NetBackup status code: 2003 .....	340
NetBackup status code: 2004 .....	341
NetBackup status code: 2005 .....	341
NetBackup status code: 2006 .....	341
NetBackup status code: 2007 .....	342
NetBackup status code: 2008 .....	342
NetBackup status code: 2009 .....	342
NetBackup status code: 2010 .....	343
NetBackup status code: 2011 .....	343
NetBackup status code: 2012 .....	343
NetBackup status code: 2013 .....	344
NetBackup status code: 2014 .....	344
NetBackup status code: 2015 .....	345
NetBackup status code: 2016 .....	345
NetBackup status code: 2017 .....	345
NetBackup status code: 2018 .....	346
NetBackup status code: 2019 .....	346

NetBackup status code: 2020 .....	346
NetBackup status code: 2021 .....	346
NetBackup status code: 2022 .....	347
NetBackup status code: 2023 .....	347
NetBackup status code: 2024 .....	347
NetBackup status code: 2025 .....	348
NetBackup status code: 2026 .....	348
NetBackup status code: 2027 .....	349
NetBackup status code: 2028 .....	349
NetBackup status code: 2029 .....	349
NetBackup status code: 2030 .....	350
NetBackup status code: 2031 .....	350
NetBackup status code: 2032 .....	351
NetBackup status code: 2033 .....	351
NetBackup status code: 2034 .....	351
NetBackup status code: 2035 .....	352
NetBackup status code: 2036 .....	352
NetBackup status code: 2037 .....	352
NetBackup status code: 2038 .....	353
NetBackup status code: 2039 .....	353
NetBackup status code: 2040 .....	353
NetBackup status code: 2041 .....	354
NetBackup status code: 2042 .....	354
NetBackup status code: 2043 .....	354
NetBackup status code: 2044 .....	354
NetBackup status code: 2045 .....	355
NetBackup status code: 2046 .....	355
NetBackup status code: 2047 .....	355
NetBackup status code: 2048 .....	355
NetBackup status code: 2049 .....	356
NetBackup status code: 2050 .....	356
NetBackup status code: 2051 .....	356
NetBackup status code: 2052 .....	357
NetBackup status code: 2053 .....	357
NetBackup status code: 2054 .....	357
NetBackup status code: 2055 .....	357
NetBackup status code: 2056 .....	358
NetBackup status code: 2057 .....	358
NetBackup status code: 2058 .....	358
NetBackup status code: 2059 .....	358
NetBackup status code: 2060 .....	359
NetBackup status code: 2061 .....	359
NetBackup status code: 2062 .....	359

NetBackup status code: 2063 .....	359
NetBackup status code: 2064 .....	360
NetBackup status code: 2065 .....	360
NetBackup status code: 2066 .....	360
NetBackup status code: 2067 .....	361
NetBackup status code: 2068 .....	361
NetBackup status code: 2069 .....	361
NetBackup status code: 2070 .....	362
NetBackup status code: 2071 .....	362
NetBackup status code: 2072 .....	362
NetBackup status code: 2073 .....	363
NetBackup status code: 2074 .....	363
NetBackup status code: 2075 .....	363
NetBackup status code: 2076 .....	364
NetBackup status code: 2078 .....	364
NetBackup status code: 2079 .....	365
NetBackup status code: 2080 .....	365
NetBackup status code: 2081 .....	365
NetBackup status code: 2082 .....	366
NetBackup status code: 2083 .....	366
NetBackup status code: 2084 .....	366
NetBackup status code: 2085 .....	367
NetBackup status code: 2086 .....	367
NetBackup status code: 2087 .....	367
NetBackup status code: 2088 .....	367
NetBackup status code: 2089 .....	368
NetBackup status code: 2090 .....	368
NetBackup status code: 2091 .....	369
NetBackup status code: 2092 .....	370
NetBackup status code: 2093 .....	370
NetBackup status code: 2094 .....	371
NetBackup status code: 2095 .....	371
NetBackup status code: 2096 .....	371
NetBackup status code: 2097 .....	372
NetBackup status code: 2098 .....	372
NetBackup status code: 2099 .....	372
NetBackup status code: 2100 .....	373
NetBackup status code: 2101 .....	373
NetBackup status code: 2102 .....	373
NetBackup status code: 2103 .....	374
NetBackup status code: 2104 .....	374
NetBackup status code: 2105 .....	374
NetBackup status code: 2106 .....	374

NetBackup status code: 2107 .....	375
NetBackup status code: 2108 .....	376
NetBackup status code: 2109 .....	376
NetBackup status code: 2110 .....	376
NetBackup status code: 2111 .....	377
NetBackup status code: 2112 .....	377
NetBackup status code: 2113 .....	377
NetBackup status code: 2504 .....	378
NetBackup status code: 2517 .....	378
NetBackup status code: 2521 .....	378
NetBackup status code: 2522 .....	379
NetBackup status code: 2523 .....	379
NetBackup status code: 2524 .....	379
NetBackup status code: 2525 .....	380
NetBackup status code: 2800 .....	380
NetBackup status code: 2801 .....	381
NetBackup status code: 2802 .....	382
NetBackup status code: 2803 .....	382
NetBackup status code: 2804 .....	384
NetBackup status code: 2805 .....	385
NetBackup status code: 2806 .....	386
NetBackup status code: 2807 .....	386
NetBackup status code: 2808 .....	387
NetBackup status code: 2809 .....	387
NetBackup status code: 2810 .....	388
NetBackup status code: 2811 .....	389
NetBackup status code: 2812 .....	390
NetBackup status code: 2813 .....	391
NetBackup status code: 2814 .....	391
NetBackup status code: 2815 .....	392
NetBackup status code: 2816 .....	392
NetBackup status code: 2817 .....	393
NetBackup status code: 2818 .....	393
NetBackup status code: 2819 .....	394
NetBackup status code: 2820 .....	394
NetBackup status code: 2821 .....	396
NetBackup status code: 2826 .....	396
NetBackup status code: 2827 .....	397
NetBackup status code: 2828 .....	397
NetBackup status code: 2829 .....	397
NetBackup status code: 2830 .....	398
NetBackup status code: 2831 .....	398
NetBackup status code: 2832 .....	398

NetBackup status code: 2833 .....	399
NetBackup status code: 2834 .....	399
NetBackup status code: 2835 .....	399
NetBackup status code: 2836 .....	400
NetBackup status code: 2837 .....	400
NetBackup status code: 2838 .....	400
NetBackup status code: 2839 .....	401
NetBackup status code: 2840 .....	401
NetBackup status code: 2841 .....	401
NetBackup status code: 2842 .....	402
NetBackup status code: 2843 .....	402
NetBackup status code: 2844 .....	402
NetBackup status code: 2845 .....	403
NetBackup status code: 2846 .....	403
NetBackup status code: 2847 .....	403
NetBackup status code: 2848 .....	403
NetBackup status code: 2849 .....	404
NetBackup status code: 2850 .....	404
NetBackup status code: 2864 .....	405
NetBackup status code: 2865 .....	405
NetBackup status code: 2866 .....	405
NetBackup status code: 4200 .....	406
NetBackup status code: 4201 .....	406
NetBackup status code: 4202 .....	407
NetBackup status code: 4203 .....	407
NetBackup status code: 4204 .....	407
NetBackup status code: 4205 .....	408
NetBackup status code: 4206 .....	408
NetBackup status code: 4207 .....	408
NetBackup status code: 4208 .....	409
NetBackup status code: 4209 .....	409
NetBackup status code: 4210 .....	410
NetBackup status code: 4211 .....	410
NetBackup status code: 4212 .....	410
NetBackup status code: 4213 .....	411
NetBackup status code: 4214 .....	411
NetBackup status code: 4215 .....	412
NetBackup status code: 4216 .....	412
NetBackup status code: 4217 .....	412
NetBackup status code: 4218 .....	412
NetBackup status code: 4219 .....	413
NetBackup status code: 4220 .....	413
NetBackup status code: 4221 .....	414

NetBackup status code: 4222 .....	414
NetBackup status code: 4223 .....	414
NetBackup status code: 4224 .....	414
NetBackup status code: 4225 .....	415
NetBackup status code: 4226 .....	415
NetBackup status code: 4227 .....	415
NetBackup status code: 4228 .....	416
NetBackup status code: 4229 .....	416
NetBackup status code: 4230 .....	416
NetBackup status code: 4231 .....	417
NetBackup status code: 4232 .....	417
NetBackup status code: 4233 .....	417
NetBackup status code: 4234 .....	418
NetBackup status code: 4235 .....	418
NetBackup status code: 4236 .....	418
NetBackup status code: 4237 .....	418
NetBackup status code: 4238 .....	419
NetBackup status code: 4239 .....	419
NetBackup status code: 4240 .....	419
NetBackup status code: 4243 .....	420
NetBackup status code: 4245 .....	420
NetBackup status code: 4246 .....	420
NetBackup status code: 4247 .....	421
NetBackup status code: 4248 .....	421
NetBackup status code: 4249 .....	421
NetBackup status code: 4250 .....	421
NetBackup status code: 4251 .....	422
NetBackup status code: 4252 .....	422
NetBackup status code: 4253 .....	422
NetBackup status code: 4254 .....	422
NetBackup status code: 4255 .....	423
NetBackup status code: 4256 .....	423
NetBackup status code: 4257 .....	424
NetBackup status code: 4258 .....	424
NetBackup status code: 4259 .....	424
NetBackup status code: 4260 .....	424
NetBackup status code: 4261 .....	425
NetBackup status code: 4262 .....	425
NetBackup status code: 4263 .....	425
NetBackup status code: 4264 .....	426
NetBackup status code: 4265 .....	426
NetBackup status code: 4266 .....	426
NetBackup status code: 4267 .....	427

NetBackup status code: 4268 .....	427
NetBackup status code: 4269 .....	427
NetBackup status code: 4270 .....	428
NetBackup status code: 4271 .....	428
NetBackup status code: 4272 .....	428
NetBackup status code: 4273 .....	428
NetBackup status code: 4274 .....	429
NetBackup status code: 4275 .....	429
NetBackup status code: 4276 .....	429
NetBackup status code: 4277 .....	430
NetBackup status code: 4278 .....	430
NetBackup status code: 4279 .....	430
NetBackup status code: 4280 .....	431
NetBackup status code: 4281 .....	431
NetBackup status code: 4282 .....	431
NetBackup status code: 4283 .....	431
NetBackup status code: 4287 .....	432
NetBackup status code: 4290 .....	433
NetBackup status code: 4293 .....	433
NetBackup status code: 4294 .....	433
NetBackup status code: 5400 .....	433
NetBackup status code: 5401 .....	434
NetBackup status code: 5402 .....	434
NetBackup status code: 5403 .....	434
NetBackup status code: 5404 .....	435
NetBackup status code: 5405 .....	435
NetBackup status code: 5406 .....	435
NetBackup status code: 5407 .....	435
NetBackup status code: 5408 .....	436
NetBackup status code: 5409 .....	436
NetBackup status code: 5410 .....	436
NetBackup status code: 5411 .....	437
NetBackup status code: 5412 .....	437
NetBackup status code: 5413 .....	437
NetBackup status code: 5414 .....	438
NetBackup status code: 5415 .....	438
NetBackup status code: 5416 .....	438
NetBackup status code: 5417 .....	438
NetBackup status code: 5418 .....	439
NetBackup status code: 5419 .....	439
NetBackup status code: 5420 .....	439
NetBackup status code: 5421 .....	439
NetBackup status code: 5422 .....	440



NetBackup status code: 5423 .....	440
NetBackup status code: 5424 .....	441
NetBackup status code: 5425 .....	441
NetBackup status code: 5426 .....	442
NetBackup status code: 5427 .....	442
NetBackup status code: 5428 .....	442
NetBackup status code: 5429 .....	443
NetBackup status code: 5430 .....	443
NetBackup status code: 5431 .....	443
NetBackup status code: 5432 .....	444
NetBackup status code: 5433 .....	444
NetBackup status code: 5434 .....	444
NetBackup status code: 5435 .....	445
NetBackup status code: 5436 .....	445
NetBackup status code: 5437 .....	445
NetBackup status code: 5438 .....	446
NetBackup status code: 5439 .....	446
NetBackup status code: 5440 .....	446
NetBackup status code: 5441 .....	447
NetBackup status code: 5442 .....	447
NetBackup status code: 5443 .....	447
NetBackup status code: 5444 .....	447
NetBackup status code: 5445 .....	448
NetBackup status code: 5446 .....	448
NetBackup status code: 5447 .....	448
NetBackup status code: 5448 .....	449
NetBackup status code: 5449 .....	449
NetBackup status code: 5450 .....	449
NetBackup status code: 5451 .....	449
NetBackup status code: 5452 .....	450
NetBackup status code: 5500 .....	450
NetBackup status code: 5501 .....	450
NetBackup status code: 5502 .....	450
NetBackup status code: 5503 .....	451
NetBackup status code: 5504 .....	451
NetBackup status code: 5505 .....	451
NetBackup status code: 5506 .....	452
NetBackup status code: 5507 .....	452
NetBackup status code: 5508 .....	452
NetBackup status code: 5626 .....	452
NetBackup status code: 5761 .....	453
NetBackup status code: 5762 .....	454
NetBackup status code: 5763 .....	454

NetBackup status code: 5764 .....	454
NetBackup status code: 5765 .....	454
NetBackup status code: 5766 .....	455
NetBackup status code: 5767 .....	455
NetBackup status code: 5768 .....	455
NetBackup status code: 5769 .....	455
NetBackup status code: 5770 .....	456
NetBackup status code: 5771 .....	456
NetBackup status code: 5772 .....	456
NetBackup status code: 5773 .....	457
NetBackup status code: 5774 .....	457
NetBackup status code: 5775 .....	457
NetBackup status code: 5776 .....	457
NetBackup status code: 5777 .....	457
NetBackup status code: 5778 .....	458
NetBackup status code: 5779 .....	458
NetBackup status code: 5780 .....	458
NetBackup status code: 5781 .....	458
NetBackup status code: 5782 .....	459
NetBackup status code: 5783 .....	459
NetBackup status code: 5784 .....	459
NetBackup status code: 5786 .....	459
NetBackup status code: 5787 .....	460
NetBackup status code: 5788 .....	460
NetBackup status code: 5789 .....	460
NetBackup status code: 5790 .....	460
NetBackup status code: 5794 .....	460
NetBackup status code: 5796 .....	461
NetBackup status code: 5798 .....	461
NetBackup status code: 5799 .....	461
NetBackup status code: 5800 .....	462
NetBackup status code: 5801 .....	462
NetBackup status code: 5803 .....	462
NetBackup status code: 5804 .....	462
NetBackup status code: 5805 .....	462
NetBackup status code: 5806 .....	463
NetBackup status code: 5807 .....	463
NetBackup status code: 5808 .....	463
NetBackup status code: 5809 .....	463
NetBackup status code: 5811 .....	464
NetBackup status code: 5812 .....	464
NetBackup status code: 5813 .....	464
NetBackup status code: 5814 .....	464

NetBackup status code: 5815 .....	465
NetBackup status code: 5816 .....	465
NetBackup status code: 5817 .....	465
NetBackup status code: 5819 .....	465
NetBackup status code: 5820 .....	465
NetBackup status code: 5821 .....	466
NetBackup status code: 5902 .....	466
NetBackup status code: 5903 .....	466
NetBackup status code: 5904 .....	467
NetBackup status code: 5905 .....	467
NetBackup status code: 5906 .....	467
NetBackup status code: 5907 .....	467
NetBackup status code: 5908 .....	468
NetBackup status code: 5909 .....	468
NetBackup status code: 5910 .....	468
NetBackup status code: 5913 .....	468
NetBackup status code: 5914 .....	469
NetBackup status code: 5915 .....	469
NetBackup status code: 5916 .....	469
NetBackup status code: 5917 .....	469
NetBackup status code: 5918 .....	470
NetBackup status code: 5919 .....	470
NetBackup status code: 5920 .....	470
NetBackup status code: 5921 .....	471
NetBackup status code: 5922 .....	471
NetBackup status code: 5925 .....	471
NetBackup status code: 5926 .....	471
NetBackup status code: 5927 .....	472
NetBackup status code: 5929 .....	472
NetBackup status code: 5930 .....	472
NetBackup status code: 5931 .....	473
NetBackup status code: 5932 .....	473
NetBackup status code: 5933 .....	473
NetBackup status code: 5934 .....	473
NetBackup status code: 5936 .....	474
NetBackup status code: 5938 .....	474
NetBackup status code: 5939 .....	474
NetBackup status code: 5940 .....	474
NetBackup status code: 5941 .....	475
NetBackup status code: 5942 .....	475
NetBackup status code: 5943 .....	475
NetBackup status code: 5944 .....	476
NetBackup status code: 5945 .....	476

NetBackup status code: 5946 .....	476
NetBackup status code: 5947 .....	476
NetBackup status code: 5948 .....	477
NetBackup status code: 5949 .....	477
NetBackup status code: 5950 .....	477
NetBackup status code: 5953 .....	478
NetBackup status code: 5954 .....	478
NetBackup status code: 5955 .....	478
NetBackup status code: 5956 .....	478
NetBackup status code: 5957 .....	479
NetBackup status code: 5958 .....	479
NetBackup status code: 5959 .....	479
NetBackup status code: 5960 .....	479
NetBackup status code: 5962 .....	480
NetBackup status code: 5963 .....	480
NetBackup status code: 5964 .....	481
NetBackup status code: 5965 .....	481
NetBackup status code: 5966 .....	481
NetBackup status code: 5967 .....	482
NetBackup status code: 5968 .....	482
NetBackup status code: 5969 .....	482
NetBackup status code: 5970 .....	483
NetBackup status code: 5971 .....	483
NetBackup status code: 5972 .....	483
NetBackup status code: 5973 .....	484
NetBackup status code: 5974 .....	484
NetBackup status code: 5976 .....	484
NetBackup status code: 5977 .....	484
NetBackup status code: 5978 .....	485
NetBackup status code: 5979 .....	485
NetBackup status code: 5980 .....	486
NetBackup status code: 5982 .....	486
NetBackup status code: 5983 .....	487
NetBackup status code: 5986 .....	488
NetBackup status code: 5987 .....	488
NetBackup status code: 5988 .....	491
NetBackup status code: 5989 .....	492
NetBackup status code: 5990 .....	493
NetBackup status code: 5991 .....	493
NetBackup status code: 5992 .....	493
NetBackup status code: 5993 .....	494
NetBackup status code: 6000 .....	494
NetBackup status code: 6530 .....	494

NetBackup status code: 6531 .....	495
NetBackup status code: 6600 .....	495
NetBackup status code: 6601 .....	495
NetBackup status code: 6602 .....	496
NetBackup status code: 6603 .....	496
NetBackup status code: 6604 .....	497
NetBackup status code: 6605 .....	497
NetBackup status code: 6606 .....	497
NetBackup status code: 6607 .....	497
NetBackup status code: 6608 .....	498
NetBackup status code: 6609 .....	498
NetBackup status code: 6610 .....	498
NetBackup status code: 6612 .....	499
NetBackup status code: 6614 .....	499
NetBackup status code: 6616 .....	499
NetBackup status code: 6617 .....	499
NetBackup status code: 6618 .....	500
NetBackup status code: 6619 .....	500
NetBackup status code: 6620 .....	500
NetBackup status code: 6621 .....	501
NetBackup status code: 6622 .....	501
NetBackup status code: 6623 .....	501
NetBackup status code: 6625 .....	501
NetBackup status code: 6626 .....	502
NetBackup status code: 6628 .....	502
NetBackup status code: 6629 .....	502
NetBackup status code: 6630 .....	503
NetBackup status code: 6631 .....	503
NetBackup status code: 6633 .....	503
NetBackup status code: 6634 .....	503
NetBackup status code: 6635 .....	504
NetBackup status code: 6640 .....	504
NetBackup status code: 6641 .....	504
NetBackup status code: 6642 .....	505
NetBackup status code: 6643 .....	505
NetBackup status code: 6644 .....	505
NetBackup status code: 6646 .....	505
NetBackup status code: 6647 .....	506
NetBackup status code: 6649 .....	506
NetBackup status code: 6650 .....	506
NetBackup status code: 6652 .....	507
NetBackup status code: 6653 .....	507
NetBackup status code: 6654 .....	507

NetBackup status code: 6655 .....	507
NetBackup status code: 7600 .....	508
NetBackup status code: 7601 .....	508
NetBackup status code: 7603 .....	508
NetBackup status code: 7604 .....	508
NetBackup status code: 7607 .....	509
NetBackup status code: 7609 .....	509
NetBackup status code: 7610 .....	509
NetBackup status code: 7611 .....	509
NetBackup status code: 7612 .....	510
NetBackup status code: 7613 .....	510
NetBackup status code: 7614 .....	510
NetBackup status code: 7617 .....	510
NetBackup status code: 7618 .....	510
NetBackup status code: 7619 .....	511
NetBackup status code: 7622 .....	511
NetBackup status code: 7623 .....	511
NetBackup status code: 7624 .....	511
NetBackup status code: 7625 .....	512
NetBackup status code: 7627 .....	512
NetBackup status code: 7628 .....	513
NetBackup status code: 7631 .....	513
NetBackup status code: 7632 .....	513
NetBackup status code: 7633 .....	514
NetBackup status code: 7634 .....	514
NetBackup status code: 7635 .....	514
NetBackup status code: 7636 .....	515
NetBackup status code: 7637 .....	515
NetBackup status code: 7638 .....	515
NetBackup status code: 7639 .....	515
NetBackup status code: 7640 .....	516
NetBackup status code: 7641 .....	516
NetBackup status code: 7642 .....	517
NetBackup status code: 7643 .....	517
NetBackup status code: 7645 .....	517
NetBackup status code: 7647 .....	518
NetBackup status code: 7648 .....	518
NetBackup status code: 7649 .....	518
NetBackup status code: 7650 .....	518
NetBackup status code: 7651 .....	519
NetBackup status code: 7652 .....	519
NetBackup status code: 7653 .....	520
NetBackup status code: 7654 .....	520

NetBackup status code: 7655 .....	521
NetBackup status code: 7656 .....	521
NetBackup status code: 7657 .....	522
NetBackup status code: 7658 .....	522
NetBackup status code: 7659 .....	522
NetBackup status code: 7660 .....	523
NetBackup status code: 8000 .....	523
NetBackup status code: 8500 .....	523
NetBackup status code: 8504 .....	524
NetBackup status code: 8505 .....	524
NetBackup status code: 8506 .....	524
NetBackup status code: 8507 .....	525
NetBackup status code: 8508 .....	525
NetBackup status code: 8509 .....	525
NetBackup status code: 8510 .....	525
NetBackup status code: 8617 .....	526
NetBackup status code: 8618 .....	526
NetBackup status code: 8619 .....	526
NetBackup status code: 8620 .....	527
NetBackup status code: 8621 .....	527
NetBackup status code: 8622 .....	527
NetBackup status code: 8623 .....	528
NetBackup status code: 8625 .....	528
NetBackup status code: 8700 .....	529
NetBackup status code: 8701 .....	529
NetBackup status code: 8702 .....	529
NetBackup status code: 8703 .....	530
NetBackup status code: 8704 .....	530
NetBackup status code: 8706 .....	530
NetBackup status code: 8707 .....	531
NetBackup status code: 8708 .....	531
NetBackup status code: 8709 .....	531
NetBackup status code: 8710 .....	531
NetBackup status code: 8711 .....	532
NetBackup status code: 8712 .....	532
NetBackup status code: 8713 .....	532
NetBackup status code: 8714 .....	532
NetBackup status code: 8715 .....	533
NetBackup status code: 8716 .....	533
NetBackup status code: 8717 .....	533
NetBackup status code: 8718 .....	534
NetBackup status code: 8719 .....	534
NetBackup status code: 8720 .....	534

NetBackup status code: 8722 .....	534
NetBackup status code: 8723 .....	535
NetBackup status code: 8724 .....	535
NetBackup status code: 8800 .....	535
NetBackup status code: 8900 .....	536
NetBackup status code: 8901 .....	536
NetBackup status code: 8902 .....	536
NetBackup status code: 9101 .....	537
NetBackup status code: 9102 .....	537
NetBackup status code: 9103 .....	537
NetBackup status code: 9300 .....	538
NetBackup status code: 9301 .....	538
NetBackup status code: 9302 .....	539
NetBackup status code: 9303 .....	539
NetBackup status code: 9304 .....	540
NetBackup status code: 9305 .....	540
NetBackup status code: 9306 .....	541
NetBackup status code: 9307 .....	541
NetBackup status code: 9308 .....	542
NetBackup status code: 9309 .....	542
NetBackup KMS status codes .....	543
NetBackup KMS status code: 1 .....	543
NetBackup KMS status code: 2 .....	543
NetBackup KMS status code: 3 .....	544
NetBackup KMS status code: 4 .....	544
NetBackup KMS status code: 5 .....	544
NetBackup KMS status code: 6 .....	544
NetBackup KMS status code: 7 .....	544
NetBackup KMS status code: 8 .....	545
NetBackup KMS status code: 9 .....	545
NetBackup KMS status code: 10 .....	545
NetBackup KMS status code: 11 .....	545
NetBackup KMS status code: 12 .....	545
NetBackup KMS status code: 13 .....	545
NetBackup KMS status code: 14 .....	546
NetBackup KMS status code: 15 .....	546
NetBackup KMS status code: 16 .....	546
NetBackup KMS status code: 17 .....	546
NetBackup KMS status code: 18 .....	546
NetBackup KMS status code: 19 .....	547
NetBackup KMS status code: 20 .....	547
NetBackup KMS status code: 21 .....	547
NetBackup KMS status code: 22 .....	547



NetBackup KMS status code: 23 .....	547
NetBackup KMS status code: 24 .....	547
NetBackup KMS status code: 25 .....	548
NetBackup KMS status code: 26 .....	548
NetBackup KMS status code: 27 .....	548
NetBackup KMS status code: 28 .....	548
NetBackup KMS status code: 29 .....	548
NetBackup KMS status code: 30 .....	548
NetBackup KMS status code: 31 .....	549
NetBackup KMS status code: 32 .....	549
NetBackup KMS status code: 33 .....	549
NetBackup KMS status code: 34 .....	549
NetBackup KMS status code: 35 .....	549
NetBackup KMS status code: 36 .....	549
NetBackup KMS status code: 37 .....	550
NetBackup KMS status code: 38 .....	550
NetBackup KMS status code: 39 .....	550
NetBackup KMS status code: 40 .....	550
NetBackup KMS status code: 41 .....	550
NetBackup KMS status code: 42 .....	551
NetBackup KMS status code: 44 .....	551
NetBackup KMS status code: 45 .....	551
NetBackup KMS status code: 46 .....	551
NetBackup KMS status code: 47 .....	551
NetBackup KMS status code: 48 .....	552
NetBackup KMS status code: 49 .....	552
NetBackup KMS status code: 50 .....	552
NetBackup KMS status code: 51 .....	552
NetBackup KMS status code: 52 .....	552
NetBackup KMS status code: 53 .....	553
NetBackup KMS status code: 54 .....	553
NetBackup KMS status code: 55 .....	553
NetBackup KMS status code: 56 .....	553
NetBackup KMS status code: 57 .....	553
NetBackup KMS status code: 58 .....	553
NetBackup KMS status code: 59 .....	554
NetBackup KMS status code: 60 .....	554
NetBackup KMS status code: 61 .....	554
NetBackup KMS status code: 62 .....	555
NetBackup KMS status code: 63 .....	555
NetBackup KMS status code: 1287 .....	555

Chapter 2	Media Manager status codes .....	556
	Media Manager status codes .....	556
	Media Manager status code 1 .....	556
	Media Manager status code 2 .....	556
	Media Manager status code 3 .....	557
	Media Manager status code 4 .....	557
	Media Manager status code 5 .....	558
	Media Manager status code 6 .....	558
	Media Manager status code 7 .....	558
	Media Manager status code 8 .....	558
	Media Manager status code 9 .....	559
	Media Manager status code 10 .....	559
	Media Manager status code 11 .....	560
	Media Manager status code 12 .....	560
	Media Manager status code 13 .....	561
	Media Manager status code 14 .....	561
	Media Manager status code 15 .....	561
	Media Manager status code 16 .....	562
	Media Manager status code 18 .....	562
	Media Manager status code 19 .....	563
	Media Manager status code 20 .....	563
	Media Manager status code 21 .....	563
	Media Manager status code 22 .....	564
	Media Manager status code 23 .....	564
	Media Manager status code 25 .....	564
	Media Manager status code 26 .....	564
	Media Manager status code 27 .....	565
	Media Manager status code 28 .....	565
	Media Manager status code 32 .....	566
	Media Manager status code 34 .....	566
	Media Manager status code 35 .....	566
	Media Manager status code 36 .....	567
	Media Manager status code 37 .....	567
	Media Manager status code 39 .....	568
	Media Manager status code 40 .....	568
	Media Manager status code 41 .....	568
	Media Manager status code 42 .....	569
	Media Manager status code 43 .....	569
	Media Manager status code 44 .....	570
	Media Manager status code 45 .....	571
	Media Manager status code 46 .....	571
	Media Manager status code 47 .....	571

Media Manager status code 48 .....	572
Media Manager status code 49 .....	572
Media Manager status code 50 .....	572
Media Manager status code 51 .....	573
Media Manager status code 52 .....	573
Media Manager status code 53 .....	574
Media Manager status code 54 .....	574
Media Manager status code 55 .....	574
Media Manager status code 57 .....	575
Media Manager status code 58 .....	575
Media Manager status code 59 .....	576
Media Manager status code 60 .....	576
Media Manager status code 61 .....	577
Media Manager status code 62 .....	577
Media Manager status code 63 .....	577
Media Manager status code 64 .....	577
Media Manager status code 65 .....	578
Media Manager status code 67 .....	578
Media Manager status code 68 .....	579
Media Manager status code 69 .....	579
Media Manager status code 70 .....	580
Media Manager status code 71 .....	581
Media Manager status code 72 .....	581
Media Manager status code 73 .....	582
Media Manager status code 74 .....	582
Media Manager status code 75 .....	582
Media Manager status code 76 .....	583
Media Manager status code 78 .....	583
Media Manager status code 79 .....	584
Media Manager status code 80 .....	584
Media Manager status code 81 .....	584
Media Manager status code 82 .....	585
Media Manager status code 83 .....	586
Media Manager status code 84 .....	586
Media Manager status code 85 .....	586
Media Manager status code 86 .....	587
Media Manager status code 87 .....	587
Media Manager status code 88 .....	587
Media Manager status code 89 .....	588
Media Manager status code 90 .....	588
Media Manager status code 92 .....	589
Media Manager status code 93 .....	589
Media Manager status code 94 .....	589

Media Manager status code 95 .....	590
Media Manager status code 96 .....	590
Media Manager status code 97 .....	591
Media Manager status code 101 .....	592
Media Manager status code 102 .....	592
Media Manager status code 104 .....	593
Media Manager status code 105 .....	593
Media Manager status code 109 .....	593
Media Manager status code 110 .....	594
Media Manager status code 111 .....	595
Media Manager status code 112 .....	595
Media Manager status code 113 .....	595
Media Manager status code 114 .....	595
Media Manager status code 115 .....	596
Media Manager status code 116 .....	596
Media Manager status code 117 .....	597
Media Manager status code 118 .....	597
Media Manager status code 119 .....	597
Media Manager status code 121 .....	598
Media Manager status code 122 .....	598
Media Manager status code 126 .....	598
Media Manager status code 127 .....	599
Media Manager status code 129 .....	599
Media Manager status code 130 .....	600
Media Manager status code 131 .....	600
Media Manager status code 132 .....	601
Media Manager status code 133 .....	601
Media Manager status code 134 .....	602
Media Manager status code 135 .....	602
Media Manager status code 136 .....	602
Media Manager status code 137 .....	603
Media Manager status code 138 .....	603
Media Manager status code 139 .....	603
Media Manager status code 140 .....	604
Media Manager status code 141 .....	604
Media Manager status code 142 .....	604
Media Manager status code 143 .....	605
Media Manager status code 144 .....	605
Media Manager status code 145 .....	605
Media Manager status code 146 .....	605
Media Manager status code 147 .....	606
Media Manager status code 148 .....	606
Media Manager status code 149 .....	606

Media Manager status code 150 .....	607
Media Manager status code 152 .....	607
Media Manager status code 153 .....	608
Media Manager status code 155 .....	608
Media Manager status code 160 .....	608
Media Manager status code 162 .....	609
Media Manager status code 163 .....	609
Media Manager status code 164 .....	609
Media Manager status code 165 .....	610
Media Manager status code 166 .....	610
Media Manager status code 167 .....	610
Media Manager status code 168 .....	611
Media Manager status code 169 .....	611
Media Manager status code 171 .....	611
Media Manager status code 172 .....	611
Media Manager status code 173 .....	612
Media Manager status code 175 .....	612
Media Manager status code 176 .....	612
Media Manager status code 177 .....	612
Media Manager status code 181 .....	613
Media Manager status code 182 .....	614
Media Manager status code 185 .....	614
Media Manager status code 186 .....	614
Media Manager status code 187 .....	615
Media Manager status code 188 .....	616
Media Manager status code 189 .....	617
Media Manager status code 190 .....	617
Media Manager status code 191 .....	618
Media Manager status code 192 .....	618
Media Manager status code 193 .....	618
Media Manager status code 194 .....	618
Media Manager status code 195 .....	619
Media Manager status code 196 .....	619
Media Manager status code 198 .....	619
Media Manager status code 199 .....	620

## Chapter 3      Device configuration status codes ..... 621

Device configuration status codes .....	621
Device configuration status code 0 .....	621
Device configuration status code 1 .....	621
Device configuration status code 2 .....	622
Device configuration status code 3 .....	622

Device configuration status code 7 .....	623
Device configuration status code 8 .....	623
Device configuration status code 9 .....	623
Device configuration status code 10 .....	623
Device configuration status code 11 .....	624
Device configuration status code 13 .....	624
Device configuration status code 14 .....	624
Device configuration status code 15 .....	625
Device configuration status code 16 .....	625
Device configuration status code 17 .....	626
Device configuration status code 18 .....	626
Device configuration status code 19 .....	626
Device configuration status code 21 .....	627
Device configuration status code 22 .....	627
Device configuration status code 24 .....	627
Device configuration status code 25 .....	628
Device configuration status code 27 .....	628
Device configuration status code 28 .....	628
Device configuration status code 29 .....	629
Device configuration status code 30 .....	629
Device configuration status code 31 .....	629
Device configuration status code 33 .....	630
Device configuration status code 34 .....	630
Device configuration status code 35 .....	630
Device configuration status code 36 .....	631
Device configuration status code 37 .....	631
Device configuration status code 38 .....	631
Device configuration status code 39 .....	631
Device configuration status code 40 .....	632
Device configuration status code 41 .....	632
Device configuration status code 42 .....	632
Device configuration status code 44 .....	632
Device configuration status code 48 .....	633
Device configuration status code 49 .....	634
Device configuration status code 51 .....	634
Device configuration status code 52 .....	634
Device configuration status code 53 .....	635
Device configuration status code 55 .....	635
Device configuration status code 56 .....	635
Device configuration status code 57 .....	636
Device configuration status code 58 .....	636
Device configuration status code 59 .....	636
Device configuration status code 60 .....	637

Device configuration status code 61 .....	637
Device configuration status code 62 .....	637
Device configuration status code 63 .....	638
Device configuration status code 64 .....	638
Device configuration status code 65 .....	638
Device configuration status code 66 .....	638
Device configuration status code 67 .....	638
Device configuration status code 68 .....	639
Device configuration status code 69 .....	639
Device configuration status code 70 .....	639
Device configuration status code 71 .....	640
Device configuration status code 72 .....	640
Device configuration status code 73 .....	640
Device configuration status code 74 .....	640
Device configuration status code 75 .....	641
Device configuration status code 76 .....	641
Device configuration status code 77 .....	641
Device configuration status code 78 .....	642
Device configuration status code 79 .....	642
Device configuration status code 81 .....	642
Device configuration status code 82 .....	643
Device configuration status code 83 .....	643
Device configuration status code 84 .....	643
Device configuration status code 85 .....	644
Device configuration status code 86 .....	644
Device configuration status code 87 .....	644
Device configuration status code 88 .....	645
Device configuration status code 89 .....	645
Device configuration status code 90 .....	645
Device configuration status code 91 .....	646
Device configuration status code 92 .....	646
Device configuration status code 93 .....	646
Device configuration status code 95 .....	647
Device configuration status code 96 .....	647
Device configuration status code 97 .....	647
Device configuration status code 98 .....	648
Device configuration status code 99 .....	648
Device configuration status code 100 .....	648
Device configuration status code 101 .....	648

Chapter 4	Device management status codes .....	649
	Device management status codes .....	649
	Device management status code 1 .....	649
	Device management status code 2 .....	649
	Device management status code 3 .....	650
	Device management status code 4 .....	650
	Device management status code 5 .....	651
	Device management status code 6 .....	651
	Device management status code 7 .....	651
	Device management status code 8 .....	652
	Device management status code 10 .....	652
	Device management status code 12 .....	653
	Device management status code 13 .....	653
	Device management status code 14 .....	653
	Device management status code 15 .....	654
	Device management status code 16 .....	654
	Device management status code 17 .....	654
	Device management status code 19 .....	655
	Device management status code 20 .....	655
	Device management status code 21 .....	655
	Device management status code 22 .....	655
	Device management status code 23 .....	656
	Device management status code 24 .....	656
	Device management status code 25 .....	657
	Device management status code 26 .....	657
	Device management status code 27 .....	657
	Device management status code 28 .....	658
	Device management status code 30 .....	658
	Device management status code 32 .....	658
	Device management status code 33 .....	659
	Device management status code 35 .....	659
	Device management status code 36 .....	660
	Device management status code 37 .....	660
	Device management status code 38 .....	660
	Device management status code 39 .....	661
	Device management status code 40 .....	661
	Device management status code 41 .....	661
	Device management status code 42 .....	662
	Device management status code 44 .....	662
	Device management status code 46 .....	662
	Device management status code 47 .....	663
	Device management status code 48 .....	663



Device management status code 49 .....	664
Device management status code 50 .....	664
Device management status code 52 .....	664
Device management status code 53 .....	665
Device management status code 55 .....	665
Device management status code 56 .....	665
Device management status code 58 .....	665
Device management status code 59 .....	665
Device management status code 60 .....	666
Device management status code 61 .....	666
Device management status code 62 .....	667
Device management status code 63 .....	667
Device management status code 64 .....	667
Device management status code 65 .....	667
Device management status code 66 .....	668
Device management status code 69 .....	668
Device management status code 70 .....	668
Device management status code 71 .....	669
Device management status code 72 .....	669
Device management status code 73 .....	669
Device management status code 74 .....	669
Device management status code 75 .....	670
Device management status code 76 .....	670
Device management status code 77 .....	670
Device management status code 78 .....	671
Device management status code 79 .....	671
Device management status code 80 .....	671
Device management status code 81 .....	672
Device management status code 82 .....	672
Device management status code 83 .....	672
Device management status code 84 .....	672

## Chapter 5      Robotic status codes ..... 673

Robotic status codes .....	673
Robotic status code 200 .....	673
Robotic status code 201 .....	673
Robotic status code 202 .....	674
Robotic status code 203 .....	675
Robotic status code 204 .....	675
Robotic status code 205 .....	675
Robotic status code 206 .....	676
Robotic status code 207 .....	676

Robotic status code 208 .....	676
Robotic status code 209 .....	677
Robotic status code 210 .....	677
Robotic status code 211 .....	678
Robotic status code 212 .....	678
Robotic status code 213 .....	679
Robotic status code 214 .....	679
Robotic status code 215 .....	679
Robotic status code 216 .....	680
Robotic status code 217 .....	680
Robotic status code 218 .....	680
Robotic status code 219 .....	681
Robotic status code 220 .....	681
Robotic status code 221 .....	681
Robotic status code 222 .....	682
Robotic status code 223 .....	682
Robotic status code 224 .....	682
Robotic status code 225 .....	683
Robotic status code 226 .....	683
Robotic status code 228 .....	684
Robotic status code 229 .....	684
Robotic status code 230 .....	684
Robotic status code 232 .....	685
Robotic status code 233 .....	685
Robotic status code 234 .....	686
Robotic status code 235 .....	686
Robotic status code 236 .....	686
Robotic status code 237 .....	687
Robotic status code 238 .....	687
Robotic status code 239 .....	687
Robotic status code 240 .....	687
Robotic status code 242 .....	688
Robotic status code 243 .....	688
Robotic status code 244 .....	688
Robotic status code 245 .....	688
Robotic status code 246 .....	689
Robotic status code 249 .....	689
Robotic status code 250 .....	690
Robotic status code 251 .....	690
Robotic status code 252 .....	690
Robotic status code 253 .....	690
Robotic status code 254 .....	690
Robotic status code 255 .....	690

Robotic status code 256 .....	691
Robotic status code 257 .....	691
Robotic status code 258 .....	691
Robotic status code 259 .....	691
Robotic status code 260 .....	692
Robotic status code 261 .....	692
Robotic status code 262 .....	692

## Chapter 6      Robotic error codes ..... 694

Robotic error codes .....	694
Robot Error status code 1 .....	694
Robot Error status code 2 .....	695
Robot Error status code 3 .....	695
Robot Error status code 4 .....	695
Robot Error status code 5 .....	696
Robot Error status code 6 .....	696
Robot Error status code 7 .....	696
Robot Error status code 8 .....	697
Robot Error status code 9 .....	697
Robot Error status code 10 .....	697
Robot Error status code 11 .....	698
Robot Error status code 12 .....	698
Robot Error status code 13 .....	698
Robot Error status code 14 .....	698
Robot Error status code 16 .....	699
Robot Error status code 17 .....	699

## Chapter 7      Security services status codes ..... 700

Security services status codes .....	700
Security services status code 93 .....	700
Security services status code 94 .....	700
Security services status code 95 .....	701
Security services status code 96 .....	701
Security services status code 97 .....	701
Security services status code 98 .....	701
Security services status code 99 .....	702
Security services status code 100 .....	702
Security services status code 101 .....	702
Security services status code 102 .....	702
Security services status code 103 .....	702
Security services status code 104 .....	703
Security services status code 105 .....	703

Security services status code 106 .....	703
Security services status code 107 .....	703

# NetBackup status codes

This chapter includes the following topics:

- [NetBackup status codes](#)
- [NetBackup KMS status codes](#)

## NetBackup status codes

The following is a complete list of the NetBackup status codes that are listed in numerical order:

---

**Note:** The term media server, as distinct from master server or server, does not apply to the NetBackup server product. When you troubleshoot a Server installation, ignore any references to media server. (This note does not apply to the NetBackup Enterprise Server.)

---

### NetBackup status code: 0

**Message:** the requested operation was successfully completed

**Explanation:** No problems were detected with the requested operation.

**Recommended Action:** No action is needed, unless a database was backed up through a database extension product (for example, NetBackup for Oracle or NetBackup for SQL Server). In those instances, code 0 means the backup script (that started the backup) ran without error. However, you must check other status as explained in the related NetBackup manual to see if the database was successfully backed up.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1

**Message:** The requested operation was partially successful

**Explanation:** A problem was detected that may require corrective action during the requested operation.

**Recommended Action:** Check the All Log Entries report and also the progress log (if there is one).

The following are some of the problems that can appear under status code 1:

- A file or a directory path is more than 1023 characters long.  
For NetBackup Snapshot Client, the maximum path name length is 1000 characters for snapshot backups, not 1023. When the snapshot is created, a new mount point is added to the beginning of the file path. If the new mount point plus the original file path exceeds 1023 characters, the backup fails with status code 1. The progress log includes the entry

```
ERR-Skipping long dir path.
```

- You cannot open a file.  
The file may have been locked for some reason.
- The following information applies only to UNIX systems:  
NetBackup cannot get the link name of a file.
- The following information applies only to UNIX systems:  
NetBackup cannot process a sparse file.
- A read error that was encountered in a file.
- File is of an unknown type, or may be hidden.
- The following information applies only to UNIX systems:  
The `lstat` system call fails on a file that is eligible to be backed up. This error may be a permission problem.
- The following information applies only to UNIX systems:  
A file cannot be locked that has mandatory locking enabled.
- A synthetic backup job may terminate with a status code 1 under the following conditions:
  - No images were found to synthesize (status code = 607).
  - TIR information has been pruned from component images (status code = 136).
  - Image format is unsupported (status code = 79).

The synthetic backup job logs the actual status code in the NetBackup error log. Refer to the documentation for the corresponding NetBackup error code for the corrective action to take.

- A BMR job may terminate with status code 1 in the following situation:  
You save the BMR configuration and it returns an error even though the child jobs completed successfully. For information, examine the **Detailed Status** tab of the **Job Details** dialog box, or the `nbjm` unified log (originator ID 117).
- A policy that contains multiple backup scripts starts a scheduled backup of a UNIX database extension client. If it fails with a status code 1, some of the backup scripts returned a failure status.
- On clients using Windows Open File Backups (WOFB) to back up open or active files, the following may occur:  
Volume snapshots were not enabled successfully for the backup.  
The following logging messages should appear in the `bpbkar32` logs if volume snapshots were not successfully enabled.  
If multistreamed backup jobs are enabled, log messages similar to the following appear that indicate volume snapshots were not enabled for the multistreamed backup job:

```
11:05:44.601 AM: [1536.724] <4> tar_backup::V_AddToFI_XBSAObj:
INF - Volume snapshots not enabled for: D:\Directory1
```

If multistreamed backups were not enabled, log messages similar to the following appear, which indicate volume snapshots were not enabled for the non-streamed backup job:

```
1:59:41.229 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF -
=====
1:59:41.229 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF - Attempting to
create snapshots for D:\Directory1
1:59:41.229 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF - CREATE request:
C:\Program Files\VERITAS\NetBackup\bin\bpfis create -fim VSP
"D:\ Directory1"
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_ParseBpfisOutput: INF - Snapshot
creation, FIS_ID: 1058813981
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_ParseBpfisOutput: INF - Snapshot creation
EXIT STATUS 11: system call failed
```

```
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF - Snapshot creation
was not successful
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF -
=====
```

In this case, examine the `bpfis` logs for error messages regarding snapshot creation failures. More details are available on the `bpfis` logs.

See the [NetBackup Snapshot Client Administrator's Guide](#).

In the `bpfis` logs, the following messages may appear when snapshot creation fails for Windows Open File Backup:

First message:

```
04:01:14.168 [376.2364] <32> onlfi-fi_split: VfMS error 11; see
following messages:
04:01:14.168 [376.2364] <32> onlfi-fi_split: Fatal method error
was reported
04:01:14.168 [376.2364] <32> onlfi-fi_split: vfm_freeze_commit:
method: VSP, type: FIM, function: VSP_make
04:01:14.168 [376.2364] <32> onlfi-fi_split: VfMS method error
3; see following message:
04:01:14.168 [376.2364] <32> onlfi-fi_split: snapshot services:
snapshot creation failed: invalid argument(s).
```

**Cause:** VSP was not enabled because the VSP snapshot for the backup did not meet the specified minimum time in the Busy File Wait VSP setting.

Either increase the Busy File Timeout VSP setting (recommended setting: 300 seconds or more) or submit the backup job when the volume has less activity.

Second message:

```
04:17:55.571 [1636.3224] <2> onlfi_vfms_logf: snapshot services:
(null): There was an unexpected error while preparing the VSP
snapshot transaction. Dumping the parameter array to provide
more information: Error 112 from VSP_Prepere
```

**Cause:** VSP was not enabled for the backup because the client for the VSP Snapshot Cache files does not have enough free disk space.

Free up disk space on the volumes being backed up.

Third message:

If Microsoft Volume Shadow Copy Service (VSS) is used as the Windows Open File Backup snapshot provider and snapshot creation fails, refer to the following: Event Viewer's Application and System Logs for error information.



- A snapshot error may have occurred. Also, you may have some clients that use the Windows Open File Backup option to back up open or active files. In this case, a log message in the `bpbkar32` debug log appears, which indicates that a snapshot error occurred.

The following is an example of a snapshot error:

```
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -
Snapshot Error while reading test.file
```

See the recommended actions under status code 156.

- The backup of Microsoft Exchange Server included multiple databases, but not all of the databases were backed up successfully. Check the job details for statements about the databases that were not backed up. In a full or a differential backup, the transaction logs are truncated for any databases that are backed up successfully. The transaction logs can be restored from the backup image even if backups of other databases fail. Warning: Any database for which the backup has failed is unprotected by this backup.
- A granular-enabled backup of Microsoft Exchange Server successfully backed up the databases, but the second GRT phase to capture mailbox-level information failed. Check the job details for the cause of the failure. In a full or differential backup, the transaction logs are truncated for any databases that are backed up successfully, regardless of whether the GRT phase succeeds. Any database that is backed up successfully can be restored from the backup image even if the GRT phase fails.
- During VMware backup, the virtual machine cannot be unlocked to allow storage migration.  
The virtual machine can be restored from this backup. However, you may want to correct this problem before the next backup.
- During VMware backup, the virtual machine snapshot cannot be deleted or the virtual machine's disks cannot be consolidated.  
The virtual machine can be restored from this backup. However, you may want to correct this problem before the next backup.
- During VMware restore, the virtual machine cannot be imported into vCloud. In the Activity Monitor, the Detailed Status tab of the job details includes messages from vCloud Director that indicate the reason for the error.  
The restored virtual machine is present on the destination vCenter. However, you must manually import it into vCloud.

A NetApp NDMP accelerator backup may terminate with a status code 1 with the following clock discrepancy warnings for the volumes:

- Clock discrepancy detected between NDMP filer and NetBackup Media Server.
- If this is not expected, please perform a backup with Accelerator forced rescan enabled.
- In order to stop seeing these messages, please address clock discrepancy.

This problem can be caused by one of the following situations:

- If the NetApp filer and NetBackup NDMP backup host have a time difference of more than 1 hour, a clock discrepancy warning is displayed for all of the volumes.  
Check the time difference for the affected volumes and update as required, or use a media server that is in the same time zone as the filer.

---

**Note:** An NTP server is the recommended method to ensure the correct time.

---

- If any SnapMirror (Data Protection) volume has a lag time of more than 1 hour, the warnings appear for that volume.  
Use the following command to determine if the volume is a Data Protection volume and if the lag time is greater than 1 hour:
  - For NetApp Clustered Data ONTAP (cDOT):  
`snapmirror show -fields lag-time`
  - For NetApp 7-mode:  
`snapmirror status`
 If Data Protection volumes are found on the filer, either:
  - Browse to and select the volumes for backup in the Backup Selections for the NetBackup policy.
  - Use the `VOLUME_EXCLUDE_LIST` with the `ALL_FILESYSTEMS` directive to exclude the mirror volumes.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2

**Message:** none of the requested files were backed up

**Explanation:** A backup or archive did not back up any of the files in the file list.

This status code applies primarily to automatic backups using Lotus Notes or SQL Server database agents, when all the backups that are job-related have failed. Or, an Enterprise Vault backup has failed. It should not occur for standard file system backups.

Open a NetBackup support case (as recommended in technical note [TECH38838](#)) if you encounter this error for a UNIX, Linux, or Windows file system backup, or for database agents other than SQL Server or Lotus Notes.

**Recommended Action:** Do the following, as appropriate:

- The following information applies only to Lotus Notes:  
This error occurs when archive style logging is not enabled for the Lotus Domino server on UNIX. It also occurs when another backup of the transaction logs is in progress.
- For troubleshooting guidance, such as a list of logs to gather, and for details on particular issues, refer to technical note [TECH38838](#).
- See the troubleshooting topic of the appropriate guide for a description of troubleshooting tools:
  - [NetBackup for Microsoft SQL Server Administrator's Guide](#)
  - [NetBackup for Lotus Notes Administrator's Guide](#)
  - [NetBackup for Enterprise Vault Agent Administrator's Guide](#)

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 3

**Message:** valid archive image produced, but no files deleted due to non-fatal problems

**Explanation:** The backup portion of the archive command reported problems so the files were not deleted.

**Recommended Action:** Examine the progress log or status of the archive on the client to determine if you need to retry the archive after you correct the problem. If the problem is not serious and the files were backed up, you can manually delete the files. To verify the files that were backed up, use the NetBackup client-user interface in restore mode and browse the files in the archive.

A possible cause for files not being deleted is that you do not have the necessary permissions. NetBackup cannot delete files unless you are the user that owns the files, a superuser on UNIX, or an administrator on Windows.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4

**Message:** archive file removal failed

**Explanation:** The backup portion of the completed archive was successful but the delete failed.

**Recommended Action:** Verify that you have permission to delete the files and that the read-only flag is not set for the files. On UNIX clients, verify that you have write permission to the directories that contain the files. Since the backup was successful, you can delete the files that were backed up. (If you do not have the necessary permissions, have the system administrator delete the files.)

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5

**Message:** the restore failed to recover the requested files

**Explanation:** Errors caused the restore to fail.

For a virtual machine restore that uses Instant Recovery, this error can occur for the following reasons:

- A name was specified incorrectly for the resource pool or temporary datastore.
- The virtual machine cannot be mounted or activated in vSphere.

**Recommended Action:** Perform the following items in the order presented:

- Ensure that the client's server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Correct the problems that you find and retry the restore.

For a virtual machine restore that uses Instant Recovery, ensure that the names for the required parameters are specified correctly. Also, check for known issues in the vSphere tasks or events. For detailed debugging, consult the `bpVMutil` logs on the restore host:

```
install_path\NetBackup\logs\bpVMutil
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6

**Message:** the backup failed to back up the requested files

**Explanation:** Errors caused the user backup to fail.

For VMware backups, this error can occur for the following reasons:

- VMware item 1: The virtual machine and the backup host virtual machine (for hotadd backup) may contain too many disks. If the total is too great for the SCSI controllers on the backup host, a backup with the hotadd transport mode fails. The following appears in the job status log:

```
ERR - Error opening the snapshot disks using given transport mode:
Status 23
```

- VMware item 2: If the VMware backup host cannot access the datastore over the selected transport mode, the backup fails. The detailed status log on the backup host may contain the following:

```
12/4/2009 1:12:34 PM - Error bpbrm(pid=21376) from client vm4: ERR
- Error opening the snapshot disks using given transport mode:
Status 23
```

- VMware item 3: Storage vMotion migrated the virtual machine's files when NetBackup performed a backup of the virtual machine directly through the ESX server.
- VMware item 4: For hotadd backups: The backup host was unable to resolve the host name of the ESX server. This error may occur if DNS is not correctly configured on the virtual machine where the backup host is installed.
- VMware item 5: For hotadd backups: If the VM to back up and the VM that contains the backup host do not reside in the same data center, the backup fails.
- VMware item 6: A previous hotadd backup of the virtual machine may have failed, as follows:
  - In hotadd backup, VMware creates a linked clone of the VM's disks and attaches the cloned disks to the backup host. (The attached disks can be seen in the vSphere Client.) If a hotadd backup of the VM fails, NetBackup may be unable to remove the cloned disks from the backup host. In the backup host, the cloned disks prevent subsequent backups from completing.
  - In a VM backup, VMware creates mount directories in the C:\Windows\Temp folder on the backup host. After the backup, VMware automatically removes

the mount directories. In some cases, such as when the backup uses the hotadd transport mode, NetBackup may be unable to remove the mount directories.

- VMware item 7: Although vSphere 6.0 supports Internet Protocol version 6 (IPv6), it does not support dual-stack configurations with both IPv4 and IPv6. (In a dual-stack network, network nodes are enabled for both IPv4 and IPv6.)

Note the following:

- If both IPv4 and IPv6 addresses are enabled, vCenter 6.0 uses IPv4 addresses only.
- If a vCenter server DNS name resolves to both IPv4 and IPv6 addresses and the IPv6 address is unreachable, note that the VMware VDDK APIs attempt to communicate over IPv6 and fail. As a result, a NetBackup backup job also fails, with status code 6.

**Recommended Action:** Do the following as appropriate:

- Verify that you have read access to the files. Check the status or the progress log on the client for messages about why the backup failed. Correct problems and retry the backup.
- The following information applies only to Windows clients:  
Verify that the account used to start the NetBackup Client service has read access to the files.
- For a UNIX or Linux database extension client (for example, NetBackup for Oracle), this status code can indicate a problem with the script that controls the backup.

Check the progress report on the client for a message such as the following:

```
Script exited with status code = number
```

The number varies. The progress log usually names the script.

Check the script for problems. Also, check the troubleshooting logs created by the database extension. See the NetBackup guide that came with the database extension for information on the scripts and the troubleshooting logs.

- VMware item 1: Add more SCSI controllers to the backup host virtual machine.
- VMware item 2: Select a different transport mode and retry the backup.
- VMware item 3: To avoid conflicts with Storage vMotion in vSphere 5.0 or later, NetBackup should conduct backups through the vCenter server. For more information, see the [NetBackup for VMware Administrator's Guide](#).
- VMware item 4: On the virtual machine, you can enter the IP address of the ESX server into the hosts file: `\Windows\System32\drivers\etc\hosts`

- VMware item 5: For a successful hotadd backup, the two virtual machines must be in the same VMware data center.
- VMware item 6: Certain mount directories or cloned disks must be manually removed to allow hotadd backups to succeed, as follows:
  - Remove the cloned disks from the VMware backup host and retry the backup.
  - Remove the mount directories from the `\Temp` folder and retry the backup. The folder name contains a string such as `VMware-System`.
- VMware item 7: Ensure that the vCenter's DNS name resolves to either an IPv4 or IPv6 address (not both).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7

**Message:** the archive failed to back up the requested files

**Explanation:** Errors caused the user archive to fail.

**Recommended Action:** Verify that you have read access to the files. Check the progress log or the status on the client for messages on why the archive failed. Correct problems and retry the archive.

On Windows clients, verify that the account used to start the NetBackup services has read access to the files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8

**Message:** unable to determine the status of `rbak`

**Explanation:** On DomainOS clients, `rbak` is used to do restores. If `rbak` does not exit with a status message, NetBackup cannot determine if the restore works.

**Recommended Action:** Check for a new core file to see if `rbak` quit abnormally. Check the `ps` output to see if `rbak` is hung. If so, cancel it and try again. Check the progress log for any unusual messages from `rbak`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9

**Message:** a necessary extension package is not installed or not configured properly

**Explanation:** A NetBackup extension product must be installed and configured to perform the requested operation.

**Recommended Action:** Verify that the required extension product is installed and configured.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 10

**Message:** allocation failed

**Explanation:** The system memory allocation fails because of insufficient system memory available. A possible cause is that the system is overloaded with too many processes and not enough physical or virtual memory.

**Recommended Action:** Free up memory by terminating any unneeded processes that consume memory. Add more swap space or physical memory.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 11

**Message:** system call failed

**Explanation:** A system call has failed. This status code is used for a generic system call failure that does not have its own status code.

**Recommended Action:** Do the following, as appropriate:

- Check the All Log Entries and Problems reports to determine the system call that failed and other information about the error.
- `nbjm` and `nbproxy` return status code 11 when an exception is processed, such as when `nbproxy` obtains policy or configuration information. Examine the `nbjm` unified log (originator ID 117) or the `nbproxy` legacy log for more detail on the cause of the error.
- A frequent cause is that the server's file system is full. For example, you may see a message similar to the following in the Problems report or `bpdbm` debug log:

```
06/27/95 01:04:00 romb romb db_FLISTsend failed: system call
failed (11)
06/27/95 01:04:01 romb romb media manager terminated by parent
process
```



```
06/27/95 01:05:15 romb romb backup of client romb that exited with
status 11 (system call failed)
```

On UNIX systems, run a `df` command on the `/usr/opensv/netbackup/db` directory.

If the `df` command does not reveal the problem, check the `bpdbm` debug logs or do a `grep` for the message

```
system call failed
```

In relevant files under the directory `/usr/opensv/netbackup/db/error/`

On Windows systems, verify that the disk partition where NetBackup is installed has enough room.

- Verify that the system is not running out of virtual memory. If virtual memory is the problem, turn off unused applications or increase the amount of virtual memory.

To increase virtual memory on Windows, do the following in the order presented:

- Display the Control Panel.
- Double-click **System**.
- On the **Performance** tab, set **Virtual Memory** to a higher value.
- The following information applies only to UNIX clients:  
 Check for a semaphore problem. This error may occur because the system does not have enough allocated semaphores. It is most commonly seen on Solaris servers when an RDBMS is also running.  
 The symptoms of the problem vary. In some cases, error messages in the NetBackup log indicate a backup failure due to an error in semaphore operation. Another symptom is the inability of the NetBackup device manager daemon, `ltid`, to acquire a needed semaphore.  
 System requirements vary; thus, no definite recommendations can be made. One customer running NetBackup and ORACLE on a Solaris server made the following changes to the `/etc/system` file and then restarted the system (`boot -r`). The changes were adequate.

```
set semsys:seminfo_semmni=300
set semsys:seminfo_semmns=300
set semsys:seminfo_semmns1=300
set semsys:seminfo_semmnu=600
```

Set these attributes to a value great enough to provide resources to all applications on your system.

- Examine other debug logs or the progress log or status on the client. Examine the `nbjm` unified log (originator ID 117) for more detail on the cause of the error.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 12

**Message:** file open failed

**Explanation:** An open of a file failed.

A disk storage unit tries to write to or create a directory on the root device of the NetBackup server or media server. In this case, the Activity Monitor job details log contains the message "not permitted to root device." By default, the absolute path or specified directory for a disk storage unit cannot be on the root file system (or system disk). You must explicitly enable them to be there when the storage unit is created.

**Recommended Action:** Do the following as appropriate:

- If you want the path for the disk storage unit to reside in the root file system: Open the **Change Storage Unit** dialog box in the **NetBackup Administration Console** and select the check box: **This directory can exist on the root file system or system disk.**
- If the specified path for the disk storage unit is not in the root file system or system device, verify that the path is in a mounted file system.
- If the specified path for the disk storage unit is in the root file system or system device but does not need to be there, use the **Change Storage Unit** dialog box to specify a different (non-root) path in a mounted file system.
- Check the NetBackup Problems report. Try to determine the file and why the error occurred. A possible cause is a permission problem with the file. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then, retry the operation and check the resulting debug log.
- For NetBackup Lotus Notes, point-in-time restore jobs may fail with a status 12. These jobs are initiated from the master server by using either the **NetBackup Administration Console** or the Backup, Archive, and Restore interface. Their failure is reported in the NetBackup tar log file. (For Windows, this file is located in the `install_path\NetBackup\logs\tar` folder. For UNIX, it is located in the `/usr/openv/netbackup/logs/tar` folder.) If the install path of the NetBackup master server is different from the install path of the NetBackup client, the automatic restore of Lotus transaction log extents during recovery of the Lotus database fail. Note that the Activity Monitor shows a status 0 (successful). The

tar log on the client, however, shows success for the restore but a failure (status 12) for the Lotus database recovery.

Perform the restore job from the Backup, Archive, and Restore interface on the NetBackup client.

- For NetBackup Snapshot Client, status code 12 may appear in the `/usr/openv/netbackup/logs/bptm` or `bpdm` log with the following:

```
tpc_read_config failed: cannot open file
/usr/openv/volmgr/database/3pc.conf
```

This status code may indicate that the policy is configured with either the NetBackup media server or the Third-party Copy Device as the off-host backup method, but the `3pc.conf` file does not exist or is in the wrong location.

Instructions are available on how to create the `3pc.conf` file.

See the [NetBackup Snapshot Client Administrator's Guide](#).

- For a FlashBackup policy, if the CACHE= entry follows the source data entry, the backup fails with status code 12. Messages such as the following appear in the `/usr/openv/netbackup/logs/bpbkar` logs on the client:

```
09:55:33.941 [6092] <16> bpfsmmap: ERR - open_snapdisk: NetBackup
snapshot enable failed error 3
09:55:33.942 [6092] <32> bpfsmmap: FTL - bpfsmmap: can't open
snapshot disk /dev/rdisk/c4t1d0s3 errno 0
09:55:33.950 [6092] <16> bpbkar Exit: ERR - bpbkar FATAL exit
status = 12: file open failed
09:55:33.956 [6092] <4> bpbkar Exit: INF - EXIT STATUS 12: file
open failed
09:55:33.957 [6092] <2> bpbkar Exit: INF - Close of stdout
complete
```

Change the order of the backup selections list so that the CACHE entry precedes the source data entry. (The source data entry specifies the raw partition that contains the file system to be backed up.)

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 13

**Message:** file read failed

**Explanation:** A read of a file or socket failed.

The possible causes include the following:

- A network communication problem that occurred on the master server, media server, or one of the clients.
- An I/O error that occurred during a read from the file system.
- Read of an incomplete file or a corrupt file.
- A socket read failure caused by a network problem or a problem with the process that writes to the socket.
- A problem specific to NetBackup Snapshot Client (see recommended actions).
- The first EV-SQL backup after a NetBackup installation failed.  
See the Troubleshooting section of the [NetBackup for Enterprise Vault Agent Administrator's Guide](#).
- On Windows, the file list that NetBackup generates for the snapshot copy operation does not have enough information to restore from the `tar32` copy. For example, block number information is not correct because the `tar32` copy is not yet created.
- NetBackup does not support the policy's **Enable file recovery from VM backup** option for dual-boot VMs.
- Locking timeouts in the VMware VDDK may cause simultaneous hotadd backups from the same VMware backup host to fail.  
In the NetBackup Activity Monitor, the detailed status log may include messages similar to the following:

```
12/05/2014 06:43:53 - begin writing
12/05/2014 06:48:53 - Error bpbrm (pid=2605) socket read failed:
errno = 62 - Timer expired
12/05/2014 06:48:55 - Error bptm (pid=2654) media manager terminated
by parent process
```

The `/NetBackup/logs/vxms` log may include repeated instances of a VDDK message similar to the following:

```
12/08/2014 05:11:35 : g_vixInterfaceLogger:libvix.cpp:1844 <DEBUG> :
[VFM_ESINFO] 2014-12-08T05:11:35.146-06:00 [7F1B1163F700 info Libs']
FILE: FileLockWaitForPossession timeout on '/var/log/vmware/hotAddLock.
dat.lck/M34709.lck' due to a local process '15882-26732358 (bpbkarv)'
```

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the problem occurred.
- Check that network communication works properly.

See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

- For a FlashBackup client, check the `/var/adm/messages` log for errors like the following:

```
Mar 24 01:35:58 bison unix: WARNING: sn_alloccache: cache
/dev/rdisk/c0t2d0s3 full - all snaps using this cache are now
unusable
```

This error indicates that the cache partition is not large enough. If possible, increase the size of the cache partition. Or, if multiple backups use the same cache, reduce the number of concurrent backups. To reduce the number, reschedule some of them or reschedule the entire backup to a time when the file system is less active.

- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.
- Ensure that the latest service packs for all products and components (SQL Server, Exchange, Notes, etc.) have been installed.
- Ensure that all the network hardware (NICs, hubs, switches, routers, etc.) throughout the environment are set to full duplex, not half duplex.
- Check the following items regarding the NICs in your system:
  - Upgrade to the latest NIC drivers throughout the system.
  - Ensure that all NICs are set to full duplex, not half duplex.  
See Troubleshooting network interface card performance in the [NetBackup Troubleshooting Guide](#).
  - Increase the timeout settings on the NIC.
  - If NIC teaming is implemented, deactivate for testing purposes.
  - Replace the NIC itself on the affected client or server.
- For NetBackup Snapshot Client, status code 13 may appear in the `/usr/openv/netbackup/logs/bpbkar` log.

The log can indicate the following:

- The files to back up reside on an IDE drive as opposed to SCSI. The off-host backup method was set to either NetBackup media server or Third-Party Copy Device. If you use off-host backup, the disk that contains the client files must be a SCSI or Fibre Channel device.  
If the disk is an IDE drive, you may see the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
get_disk_info: FTL - /var/tmp/caa026fEU disk_inquiry failed.  
Errno = 25: Inappropriate ioctl for device
```

The following listing may appear in the `/usr/openv/netbackup/logs/bpbkar` log:

```
bpbkar: INF - Processing /var  
bpbkar: ERR - get_disk_info() failed, status 13  
bpbkar: ERR - tpc_get_disk_info() failed: err 13  
bpbkar: ERR - bpbkar FATAL exit status = 13: file read failed  
bpbkar: INF - EXIT STATUS 13: file read failed
```

- The files to back up exist on a file system that is not mounted. The file system that is specified as the snapshot source must be mounted. If the snapshot source is not mounted but the mount point is present, NetBackup may try to take a snapshot of the directory preceding the directory that was specified as the snapshot source.
- For the NetBackup media server method, you may need to increase the client read timeout value. In some environments, NetBackup may require more read time than the default value allows. If the client read timeout is insufficient, the backup may fail and that causes this error.  
To increase the client read timeout for all clients, in the **NetBackup Administration Console**, go to **Host Properties > Master Servers >** double-click the master server, then go to **Properties > Timeouts**. Then, increase the client read timeout.
- On Windows, refresh the **Backup, Archive, and Restore** client console and retry the restore. This action refreshes the file list that is displayed in the client console and passes the correct information about the selected files.
- To prevent timeouts in the VMware VDDK that cause simultaneous hotadd backups from the same VMware backup host to fail, do one of the following:
  - Reduce the number of hotadd backups that run simultaneously.
  - Increase the client-read timeout on the media server as appropriate (15 minutes or more):  
In the NetBackup Administration Console, click **NetBackup Management > Host Properties >** Double-click on media server **> Timeouts > Client read timeout**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 14

**Message:** file write failed

**Explanation:** A write to a file or socket failed.

Possible causes include the following:

- An I/O error that occurred during a write to the file system.
- Write to a socket failed. The cause of this failure is a network problem or a problem with the process that reads from the socket.
- Writing to a full disk partition.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the problem occurred.
- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.
- Make sure that the routers, bridges, and other network devices are all at "full" duplex.  
See Troubleshooting network interface card performance in the [NetBackup Troubleshooting Guide](#).
- Use a "sniffer" program to determine the number of packets being rejected or re-requested.
- On Windows systems, the client `bpbkar` log may contain a 10054 Connection Reset Error (usually indicates a hardware error). Somewhere between the NetBackup client and server, the connection was reset. When NetBackup receives this error, it cannot continue the backup. This error has been attributed to the following:
  - A hiccup in the network.
  - A bad network interface card on a NetBackup client.
  - A bad network interface card on the NetBackup server.
  - Faulty routers.
  - Any other applications that interfere with NetBackup connections.
- The error occurs while you use the NetBackup Java interface: The application server (`bpjava` processes) for the NetBackup Java interface probably ran out of disk space in the file system containing `/usr/opensv/netbackup/logs/user_ops`. The application server writes temporary

files into directories in the `/user_ops` directory. Try clearing up disk space in the file system.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 15

**Message:** file close failed

**Explanation:** A close of a file or socket failed.

**Recommended Action:** Check the NetBackup Problems report for clues on where and why the problem occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 16

**Message:** unimplemented feature

**Explanation:** The specified operation is not implemented. This error should not occur through normal use of NetBackup.

**Recommended Action:** Save all error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 17

**Message:** pipe open failed

**Explanation:** Occurs in NetBackup client menu and Vault areas.

**Recommended Action:** Save all error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 18

**Message:** pipe close failed

**Explanation:** A pipe close failed when one process tries to start a child process.



**Recommended Action:** Check the NetBackup Problems report for clues on why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 19

**Message:** getservbyname failed

**Explanation:** A call to `getservbyname()` failed. The `getservbyname()` function uses the name of the service to find a service entry in the `services` file. (Or NIS services map on UNIX if it is configured.)

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on why the failure occurred.
- On a UNIX or Linux system, check that `/etc/services` and NIS services map (if applicable) have entries for the NetBackup services: `bpcd`, `bpdsm`, and `bprd`.
- On a Windows system, verify that the `%SystemRoot%\system32\drivers\etc\services` file shows the correct entries for the NetBackup Internet processes: `bpcd`, `bpdsm`, and `bprd`.  
 Ensure that the following numbers match the settings in the `services` file: The NetBackup Client Service Port number and NetBackup Request Service Port number on the **Network** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click **NetBackup Client Properties** on the **File** menu. The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.  
 See "Verifying host name and service entries" in the [NetBackup Troubleshooting Guide](#).
- Check the level of network activity. An overloaded network can cause this error.
- If these actions do not reveal the problem, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 20

**Message:** invalid command parameter

**Explanation:** One or more command parameters were not valid. This error can occur when incompatible levels of NetBackup are installed on a master and its media servers or clients. For example, a NetBackup master server has NetBackup 8.0 and the media server or the client has NetBackup 7.7.

This error can also occur if the wrong parameters are used when you run a command line.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues.
- If the error occurs when you run a command on the command line, verify that the parameters are valid.
- This status code may occur if `njbm` passes parameters but does not have a required parameter. Check the `njbm` unified logs (originator ID 117) for the list of parameters that were passed.
- The following information pertains to NetBackup Snapshot Client.
  - If the following appears in the `/usr/opensv/netbackup/logs/bptm` log as enabled on a third-party copy backup, multiplexing was enabled on a third-party copy backup:

```
bptm: cannot perform Third-Party-Copy for multiplexed backups
send_brm_msg: ERROR 20
```

bptm: EXITING with status 20

The Third-party Copy Device off-host backup method is incompatible with multiplexing (the writing of two or more concurrent backup jobs to the same storage device). You must disable multiplexing for any third-party copy backups. If multiplexing is enabled, the backup fails.

- The media server may not have the correct `3pc.conf` file entry for the client disk that is needed for the backup.

The following appears in the `/usr/opensv/netbackup/logs/bpbkar` log:

```
14:45:00.983 [15773] <4> bmap_mm_get_devid: GET_DEVICE_INDEX 1
EMC:SYMMETRIX:601092014000
14:45:00.986 [15773] <4> bpbkar child_send_keepalives: keepalive
child started, pid = 15822
14:47:02.029 [15773] <4> bmap_mm_get_devid: keepalive child:
15822 killed
14:47:02.030 [15773] <4> bmap_mm_get_devid: DEVICE_INDEX -1
14:47:02.031 [15773] <16> bmap_send_extend: ERR - can't obtain
device id string EMC:SYMMETRIX:601092014000
14:47:33.167 [15773] <16> bpbkar Exit: ERR - bpbkar FATAL exit
```

```
status = 227: no entity was found
14:47:33.167 [15773] <4> bpbkar Exit: INF - EXIT STATUS 227: no
entity was found
14:47:33.168 [15773] <2> bpbkar Exit: INF - Close of stdout
complete
```

This shows that a particular device cannot be found in the `3pc.conf` file on the media server (14:47:02.031 [15773] <16> bmap\_send\_extend: ERR - can't obtain device id string EMC:SYMMETRIX:601092014000).

The problem is one of the following:

- The `3pc.conf` file on the media server is outdated. Recreate the `3pc.conf` file.
- The media server is not on the same Fibre Channel network as the third-party copy device and client disk. As a result, the `3pc.conf` file does not have a correct entry for the client disk. Run the `bptpcinfo` command with the `-x client_name` option; this option adds the client disk to the `3pc.conf` file. For each disk that is added to the file by means of `bptpcinfo -x client_name`, you may need to add the device's World Wide Name (WWN=).

See the NetBackup Snapshot Client Configuration online document.  
 See Snapshot Client Assistance in the [NetBackup Snapshot Client Administrator's Guide](#).

- The HP VxFS snapshot mechanism requires a dedicated cache partition for each snapshot. A check is made in the mount table to make sure that the cache partition is not already in use. If the cache partition is already in use, status code 20 occurs.

Check the `/usr/opensv/netbackup/logs/bpbkar` log for a message similar to the following:

```
bpfsmap: FTL - bpfsmap: snapshot cache already in use,
/dev/arrayvg/vol4c
bpbkar Exit: ERR - bpbkar FATAL exit status = 20: invalid
command parameter
bpbkar Exit: INF - EXIT STATUS 20: invalid command parameter
```

If the snapshot cache partition is already in use, do one of the following: Set up your policy schedules to run at different times or use different cache partitions for each backup.

If the **Allow multiple data streams** option is enabled, each stream must have its own dedicated cache partition.

- Compare the NetBackup version level on the server to the version level on the clients by doing the following:
  - On UNIX or Linux NetBackup servers and clients, check the `/usr/opensv/netbackup/bin/version` file.
  - On Windows NetBackup servers, check the `install_path\Netbackup\version.txt` file or the About NetBackup item on the **Help** menu.
  - On Microsoft Windows clients, check the **About NetBackup item on the Help** menu.
  - If a Java interface displays the error, tell them how to enable the debug print manager in the Java startup file. Retry and compare the parameters that were logged on the Java log with the parameters listed in the commands usage statement.
- For the **Backup Media Server** option for VMware backups, the storage unit that is specified in the policy must be unique to your media servers. If the storage unit is also available on another media server, the snapshot job cannot succeed.
- If these actions do not reveal the problem, create a debug log directory for the process that returned this status code (if the process uses legacy logging). Then retry the operation and check the resulting log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 21

**Message:** socket open failed

**Explanation:** A socket was not opened.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that returned this status code. Then, retry the operation and check the resulting debug logs.
- The following information applies only to Sun Solaris:  
Verify that all operating system patches are installed.  
See the Operating Notes section of the [NetBackup Release Notes](#).
- The following information applies only to Windows systems:  
Verify that the recommended service packs are installed.

- The NetBackup media server may not have the Services for Network File System (NFS) installed. As a result, the media server cannot contact the Portmapper service. The attempt to manually start the NFS services fails because the Network File System is not installed.

Install the Services for Network File System on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 22

**Message:** socket close failed

**Explanation:** A socket was not closed.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting debug logs.
- The following information applies only to Sun Solaris:  
Verify that all operating system patches are installed.  
See the Operating Notes section of the [NetBackup Release Notes](#).
- The following information applies only to Windows systems:  
Verify that the recommended service packs are installed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 23

**Message:** socket read failed

**Explanation:** A read operation from a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting debug logs.
- Corrupt binaries are one possible cause for this error.  
Load a fresh `bptm` from the install media to try to resolve the problem.
- The following information applies only to Sun Solaris:

Verify that all operating system patches are installed.

See the Operating Notes section of the [NetBackup Release Notes](#).

- The following information applies only to Windows systems:  
Verify that the recommended service packs are installed.
- The NetBackup media server is an 8.0 or earlier version and you have disabled insecure communication in NetBackup. If you want to continue with the host connection, do one of the following:
  - In the **NetBackup Administration Console** on the master server host, select **Security Management > Global Security > Enable insecure communication** with the NetBackup 8.0 and earlier hosts option.
  - Specify the `nbseccmd -setsecurityconfig -insecurecommunication on` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 24

**Message:** socket write failed

**Explanation:** A write operation to a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then retry the operation and check the resulting debug logs.
- A possible cause is a high network load. For example, this problem occurs with `Cannot write to STDOUT` when a Windows system that monitors network load detects a high load. It then sends an ICMP packet to other systems to inform them that the route they use is disconnected. The log messages were similar to the following:

```
01/31/96 14:05:23 ruble crabtree.null.com from client
crabtree.null.com: ERR - Cannot write to STDOUT. Err no= 242: No
route to host
01/31/96 14:05:48 ruble crabtree.null.com successfully wrote
backup id crabtree.null.com_0823125016, copy 1, fragment 1,
440864 Kbytes at 628.538 Kbytes/sec
01/31/96 14:05:51 netbackup crabtree.null.com CLIENT
crabtree.null.com POLICY Remote3SysFullW SCHED Sirius EXIT
STATUS 24 (socket write failed)
```

- The following information applies only to Sun Solaris:  
Verify that all operating system patches are installed.  
See the Operating Notes section of the [NetBackup Release Notes](#).
- The following information applies only to Windows systems:  
Verify that the recommended service packs are installed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 25

**Message:** cannot connect on socket

**Explanation:** A process that timed out while it connects to another process for a particular operation. This problem can occur in the following situation: when a process tries to connect to the NetBackup request daemon (`bprd`) or database manager daemon (`bpdbm`) and the daemon is not running. (On Windows, these daemons are the NetBackup Request Manager and the NetBackup Database Manager services.)

It can also occur in the following situations: the network or server is heavily loaded and has slow response time or an evaluation license key for NetBackup expired. However, the most common cause of this error is a host name resolution problem.

The following are other possible causes of this error caused by network connectivity issues or a required process such as `pbx_exchange` not running.

- `nbjm` is unable to connect to `bpcd` on the media server
- `nbpem` is unable to connect to `nbproxy`
- `bptm` on the media server is unable to connect to `nbjm` on the master server.
- You cannot perform an immediate backup operation.

These errors are caused either by network connectivity issues or if a required process such as `pbx_exchange` is not running.

**Recommended Action:** Do the following, as appropriate:

- Verify that `bpcmpatd`, `vnetd`, and Private Branch Exchange (PBX) are running.  
Information on how to start PBX is available.  
See "Resolving PBX problems" in the [NetBackup Troubleshooting Guide](#).
- If necessary, stop and restart NetBackup.
  - On UNIX systems, enter the following:

```
/usr/opensv/netbackup/bin/bp.kill_all
/usr/opensv/netbackup/bin/bp.start_all
```

- On Windows systems, enter the following:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

- The following information applies only to a UNIX or Linux NetBackup master server:  
Verify that the `bprd` and the `bpbdbm` processes are running. If these processes are not running, start them. On a Windows master server, verify that the NetBackup Request Manager and the NetBackup Database Manager services are running. If these services are not running, start them.  
If these processes or services are running, examine the All Log Entries report for the time of the failure to determine where the failure occurred.  
Do one of the following:
  - If you cannot view the report or you get a `cannot connect on socket error`, verify again that the NetBackup Database Manager service or daemon is running. Then, create a debug log directory for `bpbdbm`, retry the operation, and check the resulting debug log.
  - If you view the report and do not find a problem-related entry, create the debug log directories for the related processes that were running when the error first appeared. (This process frequently is `bpbbrm`.) Then, retry the operation and check the resulting debug logs.
- Verify that the server list specifies the correct master server.
  - The following information applies only to Windows systems:  
The master server is designated in the **Server to use for backups and restores** drop-down in the **Specify NetBackup Machines and Policy Type** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click **Specify NetBackup Machines and Policy Type** on the **File** menu.
  - The following information applies only to UNIX and Linux systems:  
The master server is the first `SERVER` entry in the `bp.conf` file.
  - Check the following Veritas Support website to ensure that all recommended NetBackup patches are installed:  
[www.veritas.com/support](http://www.veritas.com/support)
  - If failure occurs when you run a user-directed backup from a client, make sure that a user-directed backup schedule exists at the master server.
  - With NetBackup database extensions:  
Make sure that the applicable database product has the correct permissions allowing NetBackup to write to the progress log on the client.



- The following information applies only to UNIX systems:  
 If `bpdbm` has quit when the shutdown script runs on a media server, carefully read the `K77netbackup` script. It contains details on how to prevent this problem. The script is in `/usr/openv/netbackup/bin/goodies`.  
 If you change the server list on a master server, stop, and restart the following: The NetBackup Database Manager and request daemons (UNIX) or the NetBackup Database Manager and NetBackup Request Manager services (Windows).
- Check the `services` file.
  - The following information applies only to UNIX systems:  
 Verify that the `/etc/services` file (and NIS services if NIS is used) has entries for the NetBackup services: `bpcd`, `bpdbm`, and `bprd`.  
 On Windows, verify that the `%SystemRoot%\system32\drivers\etc\services` file has the correct entries for `bpcd`, `bpdbm`, and `bprd`.  
 Also, verify that the following numbers match the settings in the `services` file: The **NetBackup Client Service Port** and the **NetBackup Request Service Port** on the **Network** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click **NetBackup Client Properties** on the **File** menu. The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.  
 See Verifying host names and service entries in NetBackup in the [NetBackup Troubleshooting Guide](#).
- On Sun Solaris, verify that all operating system patches are installed  
 See the Operating Notes section of the [NetBackup Release Notes](#).
- On Windows, verify that the recommended service packs are installed.
- When the base NetBackup license key expires, daemons (such as `bprd` and `bpdbm`) terminate on the NetBackup server. If these daemons are not running, you are likely to encounter status code 25 errors in the Administration console. Install a valid base NetBackup license key, restart the daemons, and restart the console.
- For NetBackup Snapshot Client, the following applies: When many devices are configured on a media server, it may take a long time for the `bptpcinfo` command to generate the file `3pc`. When the backup is run for the first time, the backup may fail with status 25. Make sure that the `/usr/openv/volmgr/database/3pc.conf` file exists. If it does, rerun the backup. If the backup fails again, run the `bptpcinfo` manually to generate the file `3pc`, then try the backup again.

- In the Auto Image Replication (A.I.R.) scenario, the error can occur if insecure communication is disabled in NetBackup after the trust relationship between the 8.1 and 8.0 master servers is established. If you want to continue with the host connection, do one of the following:
  - In the **NetBackup Administration Console** on the master server host, select the **Security Management > Global Security > Secure Communication > Enable insecure communication with NetBackup 8.0 and earlier hosts** option.
  - Specify the `nbseccmd -setsecurityconfig -insecurecommunication on` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 26

**Message:** client/server handshaking failed

**Explanation:** A process on the server encountered an error when it communicated with the client. This error indicates that the client and server were able to initiate communications, but encountered difficulties and the communications did not complete. This problem can occur during a backup or a restore.

**Recommended Action:** Determine which activity encountered the handshake failure by examining the All Log Entries report for the appropriate time period. Determine the client and server that had the handshake failure.

For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 27

**Message:** child process killed by signal

**Explanation:** A child of the process that reported this error was terminated. This error may occur if the backup job was terminated or another error terminated the child process. This problem may also occur if a NetBackup process was terminated through Task Manager or another utility.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create

a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 28

**Message:** failed trying to fork a process

**Explanation:** A fork of a child process failed (on UNIX) or a `CreateProcess` failed (on Windows).

This failure may be due to the following:

- An overloaded system
- Insufficient swap space or physical memory
- Too many processes are running on the system

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create debug log directories for the processes that think may have returned this status code. Then, retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 29

**Message:** failed trying to exec a command

**Explanation:** A command was not run. This error can occur because the permissions of the command do not allow it to be run. Or it occurs due to a lack of system resources such as memory and swap space.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup All Log Entries report for clues on where and why the failure occurred.
- Check the permissions on the command to be run.
- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 30

**Message:** cannot get password information

**Explanation:** Could not get the `passwd` entry for a user.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 31

**Message:** could not set user ID for process

**Explanation:** Could not set the user ID of a process to the user ID of the requesting user. NetBackup runs client processes as the requesting user.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 32

**Message:** could not set group ID for process

**Explanation:** Could not set the group ID of a process to the requesting user group. NetBackup runs client processes with the group ID of the requesting user.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 33

**Message:** failed while trying to send mail

**Explanation:** An email notification about backup, archive, or restore results has failed. The email was not sent to the administrator's address as specified by the email global attribute. On a UNIX or Linux client, the email was not sent to an email address that is specified with USEMAIL in the client's `bp.conf` file.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 34

**Message:** failed waiting for child process

**Explanation:** A NetBackup process encountered a failure while it waited for a child process to complete.

**Recommended Action:** Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 35

**Message:** cannot make required directory

**Explanation:** Could not create a required directory.

Possible causes are the following:

- A process does not have permission to create the directory
- The path to the directory is not valid
- An IO error occurs
- No space is available on the device that contains the directory

For Hyper-V, Hyper-V servers or SCVMM servers with IPv6 addresses are not supported. For VMware, using IPv6 addresses to refer to NetBackup clients are not supported.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup All Log Entries report to determine which directory was not created and why it was not created. In particular, check for a full disk partition.
- Check the permissions on the parent directory. Verify that NetBackup services are started with a **Logon as** account that has permission to create the directory.
- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 36

**Message:** failed trying to allocate memory

**Explanation:** Allocation of system memory failed. This error occurs when an insufficient system memory is available. The system may be overloaded with too many processes and it does not have enough physical and virtual memory.

**Recommended Action:** Free up memory by terminating any unneeded processes that consume a lot of memory. Add more swap space or physical memory.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 37

**Message:** operation requested by an invalid server

**Explanation:** An invalid media server or Windows NetBackup Remote Administration Console made a request to the NetBackup request daemon (`bprd`) or NetBackup Database Manager daemon (`bpdbm`). On Windows, these daemons are the NetBackup Request Manager and NetBackup Database Manager services.

**Recommended Action:** Examine the NetBackup All Log Entries report for the time of this error to determine which system tried to connect to the master server.

If the server is a valid media server, verify that the storage unit for the media server is defined. Also, verify that the server or Windows NetBackup Remote Administration Console has a server list entry on the master server.

If necessary, update the server list.

On a UNIX or Linux master server, add a `SERVER = media_server_name` to the `bp.conf` file. `media_server_name` is the host name of the media server. On a Windows master server, add the media server to the list on the **Servers** tab in the **Master Server Properties** dialog box.

See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

If a server or Windows NetBackup Remote Administration Console has more than one host name (for example, multiple network interfaces), verify that the master server has a server list entry for each of them.

If you change the server list on a UNIX or Linux master server, for the changes to take effect do the following: stop and restart the NetBackup Request daemon (`bprd`) and NetBackup Database Manager daemon (`bpdbm`). If you change the server list on a Windows master server, stop, and restart the NetBackup Request Manager and NetBackup Database Manager services.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 38

**Message:** could not get group information

**Explanation:** Could not get the group entry that describes a UNIX or Linux user group.

**Recommended Action:** Check the NetBackup Problems report for clues on why the error occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 39

**Message:** client name mismatch

**Explanation:** The client used a name in a request to the NetBackup server that did not match the configured name in the policy on the server.

**Recommended Action:** Change one of the following so the two match: the NetBackup client name setting on the client (see the applicable NetBackup users guide) or the one in the policy configuration on the server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 40

**Message:** network connection broken

**Explanation:** The connection between the client and the server was broken. This status code can also appear if the connection is broken between the master and the media server during a backup.

**Recommended Action:** Do the following, as appropriate:

- Try pinging the client from the server. If pinging is not possible, check for loose connections or other network problems.
- Verify that the server list settings are correct on both the client and the server. If the backup involves a media server, verify that these entries are correct on both the master and the media server. For example, if a media server does not have a server list entry for the master, it does not accept connections from the master.
  - On Windows, the master server is designated on the **Servers** tab in the **Master Server Properties** dialog box.  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
  - On UNIX and Linux systems, the master server is the first `SERVER` entry in the `bp.conf` file.

If you change the server list on a UNIX or Linux master server, you must stop and restart the NetBackup Request daemon (`bprd`) and NetBackup Database Manager daemon (`bpdbm`) in order for the changes to take effect. On Windows, stop and restart the NetBackup Request Manager and NetBackup Database Manager services.

- Status code 40 can also be due to denial of a mount request by the operator.
- This status code may occur if `nbjm` was unable to connect to `bpbm` or to `bpmount`. Examine the `nbjm` unified log (originator ID 117) or the `bpbm` or the `bpmount` legacy logs for more detail on the cause of the error.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 41

**Message:** network connection timed out

**Explanation:** The possible causes include the following:

- The server did not receive any information from the client for too long a period of time.
- You have attempted to back up too many files using FSCP (File level fast single copy backup) with fast backup enabled.



- NetBackup uses the available bandwidth to its maximum potential and pushes the requests accordingly; however, the Amazon S3 compliant cloud cannot process the high number of requests.

The cloud vendor returns error 503 to slow down the requests and the backup job fails with the following errors:

In the media server, `bptm` logs the following:

```
bptm:4940:<media_server_name>: AmzResiliency:
AmzResiliency::getRetryType cURL error: 0, multi cURL error: 0,
HTTP status: 503, XML response: SlowDown, RetryType: RETRY_EXHAUSTED
```

In the media server, `bpbrm` logs the following:

```
bpbrm Exit: client backup EXIT STATUS 41: network
connection timed out
```

This issue occurs only if a higher bandwidth is available between NetBackup and the cloud storage.

**Recommended Action:** Do the following, as appropriate:

- If you back up too many files, use **Host Properties** on the NetBackup server to change **Client read timeout** to a much higher value (e.g., 4000). These settings are on the **Universal Settings** tab in the **Master Server Properties** dialog box. The default for this timeout is 300 seconds.

Also, set the **File browse timeout** on the **Timeouts** tab to a value greater than 4000.

Then retry the operation. The names of the files are logged on the debug log file in the `/usr/openv/netbackup/logs/bpbkar` directory before `bpbkar` processes them. The last file in the log is the file that causes problems.

- On UNIX, Linux, or Windows clients, check for the following problems with the `bpbkar` client process.

On Windows clients: The `bpbkar` client process is not hung. Due to the files and directories it scans, it has not replied to the server within the **Client read timeout** period. This error occurs during incremental backups when directories have thousands of unmodified files.

For this case, use **Host Properties** on the NetBackup server to change **Client read timeout**. This setting is on the **Universal Settings** tab in the **Master Server Properties** dialog box. The default for this timeout is 300 seconds.

See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

You can also monitor CPU utilization to determine if this condition exists.

The following information applies only to UNIX or Linux clients:

- The `bpbkar` client process is hung on a file that has a mandatory locking set. For this case, add the following to the client's `bp.conf` file:

```
VERBOSE
```

And as root on the client run the following:

```
touch /usr/opensv/netbackup/bpbkar_path_tr
/usr/opensv/netbackup/logs/bpbkar
```

Then retry the operation. The names of the files are logged on the debug log file in the `/usr/opensv/netbackup/logs/bpbkar` directory before `bpbkar` processes them. The last file in the log is the file that causes problems.

---

**Note:** Also, use these procedures for other unknown `bpbkar` hangs.

---

If the problem is due to mandatory file locking, have NetBackup skip the locked files. Set `LOCKED_FILE_ACTION` to `SKIP` in the `/usr/opensv/netbackup/bp.conf` file on the client.

- The `bpbkar` client process is not hung. Due to the files and directories it scans, it has not replied to the server within `CLIENT_READ_TIMEOUT` or `CLIENT_CONNECT_TIMEOUT`. This error occurs during backups when directories have thousands of unmodified files or during restores of the sparse files that have thousands of holes. For this case, try to add or modify the `CLIENT_READ_TIMEOUT` value in the server's `/usr/opensv/netbackup/bp.conf` file. The default for `CLIENT_READ_TIMEOUT` is 300 seconds if it is not specified.

Use your system's `ps` command and monitor CPU utilization to help decide which of these conditions exist.

When you finish the investigation of the problem, delete the `/usr/opensv/netbackup/logs/bpbkar` directory, since the log files can become quite large and are not deleted automatically. Also delete `/usr/opensv/netbackup/bpbkar_path_tr` so you do not generate larger log files than needed the next time you create directory `/usr/opensv/netbackup/logs/bpbkar`.

- On Windows systems, try the following:
  - Disable the following file:
 

```
install_path\VERITAS\NetBackup\bin\tracker.exe
```
  - Repair hard drive fragmentation. Try an application that is called Diskeeper Lite, which is part of the Windows Resource Kit.

- Make sure that enough space is available in `\temp`.
- If the server cannot connect to the client, create `bpcd` or `bpbkar` (UNIX, Linux, and Windows only) debug log directories on the client. Then retry the operation and check the resulting logs. If these logs do not provide a clue, create a `bpbrm` debug log on the server. Then retry the operation and check the resulting debug log.

If the `bpbrm` log has entries similar to the following, the problem is in the routing configuration on the server:

```
bpbrm hookup_timeout: timed out waiting during the client hookup
bpbrm Exit: client backup EXIT STATUS 41: network connection
timed out
```

Verify that the client IP address is correct in the name service that is used. On UNIX clients, if both the NIS and the DNS files are used, verify that they match. See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

- If you use an AIX token ring adapter and the `routed` daemon is running, the timeout occurs because the token ring adapter creates dynamic routes. It then causes the `routed` daemon to crash.
- For a FlashBackup client, this error occurs if the file system being backed up is very large and has a very large number of files. It can also occur if a large number of concurrent data streams are active at the same time. To correct it, add `CLIENT_READ_TIMEOUT` to the `/usr/opensv/netbackup/bp.conf` file and set it to increase the timeout interval.
- Make sure all recommended NetBackup patches are installed. Check the following Veritas Support website for current patch information:  
[www.veritas.com/support](http://www.veritas.com/support)
- Add the `CLIENT_READ_TIMEOUT` values to the master server, media server, and client when a NetBackup database extension product is installed. The values should all be the same for each server. The value set is dependent on the size of the database being backed up. More information on `CLIENT_READ_TIMEOUT` is available.  
See the [NetBackup Administrator's Guide, Volume II](#).
- Make sure that enhanced authentication is configured correctly. For example, the following may result in status code 41: Host A is configured to use enhanced authentication with host B, but host B is not configured to use enhanced authentication with host A. In this case, connections from host B to host A are likely to fail with status code 41. Connections from host A to B are likely to fail with authentication errors (status code 160).

- If the Amazon S3 compliant cloud is not able to process the high number of requests, perform one of the following:
  - Configure the bandwidth throttling to reduce the number of requests. See "NetBackup cloud storage server connection properties" in the [NetBackup Cloud Administrator's Guide](#).
  - Reduce the number of read/write buffers. See "NetBackup cloud storage server bandwidth throttling properties" in the [NetBackup Cloud Administrator's Guide](#).
  - Ask your cloud vendor to increase the parallel requests limit.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 42

**Message:** network read failed

**Explanation:** An attempt to read data from a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Verify that both the client and the server are operational.
- Resolve any network communication problems.  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- Check the Problems report for clues.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 43

**Message:** unexpected message received

**Explanation:** The client and the server handshake were not correct.

**Recommended Action:** Do the following, as appropriate:

- Verify that the correct version of software is running on the client and the server.
- To enable detailed debug logging, do the following:
  - On the server, create a `bpbrrm` debug log directory.
  - On clients, create a `bpcd` debug log directory.
  - Increase the amount of debug information to include in the logs.

See "About logs" in the [NetBackup Logging Reference Guide](#).

- Retry the operation and examine the logs.  
If you use `bpstart_notify` scripts on UNIX, Linux, or Windows clients, verify that messages are not written to `stdout` or `stderr`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 44

**Message:** network write failed

**Explanation:** An attempt to write data to a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Check the Problems report for information about the error.
- Verify that the client and servers are operational and connected to the network.
- Create a debug log directory for the process that reported the problem and the operation. Examine the resulting debug log file for detailed troubleshooting information.

See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 45

**Message:** request attempted on a non-reserved port

**Explanation:** A try was made to access a client from a non-reserved port.

**Recommended Action:** Verify that the latest software is installed on the client and server.

- On UNIX NetBackup servers and clients, check the `/usr/opensv/netbackup/bin/version` file.
- On Windows NetBackup servers, check the `install_path\netbackup\version.txt` file or the **About NetBackup** item on the **Help** menu.
- On Microsoft Windows clients, check the **About NetBackup** item on the **Help** menu.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 46

**Message:** server not allowed access

**Explanation:** The server tries to access a client, but access is blocked.

Possible causes are as follows:

- The server is not listed on the client as a valid server.
- The client was configured to require encrypted backups, but the encryption attribute for the backup policy on the server was not selected.
- The evaluation license for the NetBackup Encryption product has expired on the server, but the NetBackup client was configured to require encrypted backups. As a result, the server tries to make a non-encrypted backup of the client. Since the client is configured to require encryption, the backup failed.

**Recommended Action:** Do the following, as appropriate:

- If the server is a valid server but is not listed on the client, add its name to the client's server list:
  - On Windows clients in the **Specify NetBackup Machines and Policy Type** dialog box, do the following: Add the server in the **Server to use for backups and restores** drop-down list. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click **Specify NetBackup Machines and Policy Type** on the **File** menu.
  - On UNIX and Linux clients, add a `SERVER` entry in the `bp.conf` file.

If you continue to have problems, more information is available:

See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

See "Verifying host names and services entries" in the [NetBackup Troubleshooting Guide](#).

- To make non-encrypted backups of the client, set `CRYPT_OPTION` on the client to **allowed** or **denied**.  
Refer to the [NetBackup Security and Encryption Guide](#).
- If the NetBackup encryption evaluation license has expired on the server and you want to continue encrypting backups of the client, do the following: Purchase a permanent encryption license key and add it to the server. After you add the permanent encryption license key, check the attributes of the backup policy to make sure that encryption is selected.

To check the validity of an evaluation license key, do the following:

On Windows, go to the **Help** menu on the **NetBackup Administration** window on the NetBackup server and select **License Keys**. If the evaluation key is not

listed in the **NetBackup License Keys** window, the key has expired. Use this window to add the new permanent encryption key.

On UNIX, use the following command on the server:

```
/usr/opensv/netbackup/bin/admincmd/get_license_key
```

Select option `f` to list the active license keys and features. If the evaluation key is not listed, the key has expired. Use this command to add the new permanent encryption key.

- Be sure that all name resolution services (primary, load-balancing, and secondary) are properly configured for consistent forward and reverse name resolution of NetBackup hosts.

More information is available in the following technical article:

<http://www.veritas.com/docs/TECH204794>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 47

**Message:** host is unreachable

**Explanation:** An attempt to connect to another computer failed.

**Recommended Action:** Do the following, as appropriate:

- Verify that the name service (or services) used by the client are configured to resolve the host names of the NetBackup server correctly.
- Verify that the name service (or services) used by the server are configured to resolve the host name of the NetBackup client correctly.
- Try to ping the client from the server and the server from the client.
- If you continue to have problems, do the following:  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 48

**Message:** client host name could not be found

**Explanation:** The system function `gethostbyname()` failed to find the client's host name.

**Recommended Action:** Verify that the client name is correct in the following:

- The NetBackup policy configuration on the master server.
- The **General** tab in the following dialog boxes: **NetBackup Client Properties** and **Specify NetBackup Machines and Policy Type** (on Microsoft Windows non-target clients). To display these dialog boxes, start the Backup, Archive, and Restore interface on the client. For the **General** tab, click **NetBackup Client Properties** on the **File** menu; click **Specify NetBackup Machines and Policy Type** on the **File** menu.
- The `bp.conf` file on UNIX and Linux clients.
- On clients and servers, verify that the name service is set up to resolve the NetBackup client names correctly.  
On UNIX clients, verify that the client's host name is in the `/etc/hosts` file or the YP hosts file or NIS maps.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 49

**Message:** client did not start

**Explanation:** The client failed to start correctly.

**Recommended Action:** Do the following, as appropriate:

- Make sure that software is installed on the client and it is the correct version. If necessary, reinstall the client software.
- Check for full file systems on the client.
- Enable detailed debug logging on the client by doing one of the following:
  - Create `bpcd` and `bpbkar` (UNIX, Linux, and Windows only) debug log directories.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On Windows clients, increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the resulting logs.
- On UNIX or Linux systems, use the UNIX `sum` command to check for corrupt binaries.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 50

**Message:** client process aborted

**Explanation:** One of the following has occurred:

- The client backup terminates abnormally. For example, a NetBackup master or media server is shutdown or restarted when a backup or restore is in progress.
- An administrator uses an OS-provided command line (for example, the kill command) to kill an active process. The job status does not reflect the change until one hour later, when the status changes to DONE and this status code is generated.

**Recommended Action:** Do the following, as appropriate:

- Enable detailed debug logging.
  - Create a `bpbkar` debug log directory (UNIX, Linux, and Windows clients only).
  - Create a `bpcd` debug log directory.
  - On UNIX clients, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).

Retry the operation and examine the resulting logs.

- This error may occur if `nbjm` terminated while a backup job was running. Examine the unified logging files on the NetBackup server for `nbjm` (117) for more detail on the error. All unified logging is written to `/usr/openv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- On UNIX clients, check for core files in the `/` directory.
- On UNIX clients, check the system log (`/usr/adm/messages` on Solaris) for system problems.
- This problem can sometimes be due to a corrupt binary.  
On UNIX clients, use the UNIX `sum` command to check the `bpcd`, `bpbkar`, and `tar` binaries, which are located in `/usr/openv/netbackup/bin` on the client. Reinstall them if they are not the same as in the client directory under `/usr/openv/netbackup/client` on the server.  
On a Windows client, check the `bpinetd.exe`, `bpcd.exe`, `bpbkar32.exe`, and `tar32.exe` files, which are located in the `install_path\NetBackup\bin` folder on the client.

Reinstall the client if these files are as follows:

- Not the same size as on other Windows clients
- Not at the same release level
- Do not have the same NetBackup patches as other Windows clients

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 51

**Message:** timed out waiting for database information

**Explanation:** The catalog process did not respond within five minutes.

**Recommended Action:** Do the following, as appropriate:

- Verify that the NetBackup Database Manager service or daemon is running.
- Verify that the file system that contains the NetBackup catalogs has enough space.
- Create `bpbrm` and `bpdbm` debug log directories on the server and retry the operation.
- Look in the debug log files to find more information on the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 52

**Message:** timed out waiting for media manager to mount volume

**Explanation:** The requested volume was not mounted before the timeout expired. This error can also occur if the volume is a cleaning tape but was not specified as a cleaning tape.

Another possible cause: the last available drive has a mount request for a non-backup (such as a restore). Then a backup that requires the same drive is initiated before the mount completes. This error is due to the drive not being reported as busy until the mount completes.

**Recommended Action:** Do the following, as appropriate:

- Verify that the requested volume is available and an appropriate drive is ready and in the UP state.

- If this error occurs during a read operation (restore, duplicate, verify), the drives could be busy. Increase the timeout for the media mount that the NetBackup global attribute specifies, to allow more time to mount and position the media.
- Verify that the tape is not a cleaning tape that is configured as a regular volume.
- When an Automated Cartridge System controls the robot, verify that the ACSLS system is up.
- If it is an initial installation, a procedure is available.  
See "Troubleshooting configuration problems" in the [NetBackup Troubleshooting Guide](#).
- On Windows, check the Event Viewer Application log for the error messages that indicate why the tape mount did not complete. On UNIX, check the system log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 53

**Message:** backup restore manager failed to read the file list

**Explanation:** The backup and restore manager (`bpbrm`) did not read the list of files to back up or restore.

**Recommended Action:** Verify that the server software was installed correctly on all NetBackup servers. If that is not the problem, do the following:

- Create `bpbrm` debug log directories on the server.
- On a UNIX or Linux NetBackup server, add the `VERBOSE` option to the `bp.conf` file. On a Windows NetBackup server, set the **Global logging level** option on the **Logging** tab in the **Master Server Properties** dialog box.  
To display this dialog box, refer to the following topic:  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).  
Increase the unified logging levels by using the `vxlogcfg` command as explained in the following procedure:  
See "About unified logging" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug logs for detailed troubleshooting information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 54

**Message:** timed out connecting to client

**Explanation:** The server did not complete the connection to the client. The accept system or Winsock call timed out after 60 seconds.

Some third-party software packages (for example, a personal firewall product) can affect the TCP/IP stack in Windows. This action can cause a loss of connection between the NetBackup server and the `bpcd` process on the client. NetBackup tries to set `SO_REUSEADDR` (allows local address reuse) on the inbound socket connection so that the port can be handed off from `bpinetd.exe` (the NetBackup Client Service) to `bpcd.exe`. Some products may not allow this functionality due to the various methods that can be used to violate system security.

**Recommended Action:** Do the following, as appropriate:

- Perform the following procedure:  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- On UNIX clients, verify that the `/usr/opensv/netbackup/bin/bpcd` binary exists and that it is the correct size.
- Check the `/etc/inetd.conf` file to make sure the `bpcd` path is correct in the following entry:

```
bpcd stream tcp nowait root /usr/opensv/netbackup/bin/bpcd bpcd
```

- On the systems that include the following, make sure that the client name is in the master's `/etc/hosts` file: NetBackup master, media, and clients (with NetBackup database extension products installed on one or more clients).
- Completely uninstall the third-party software package on the client that causes the failure. Or, contact the software manufacturer to investigate if other configuration options or workarounds are possible.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 55

**Message:** permission denied by client during `rcmd`

**Explanation:** The UNIX or Linux client does not have the server's name in its `/.rhosts` file.

**Recommended Action:** Add the server name to the `/.rhosts` file on the UNIX or Linux client.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 56

**Message:** client's network is unreachable

**Explanation:** The client cannot reach the host (WSAENETUNREACH on Windows or ENETUNREACH on UNIX) on a system call.

**Recommended Action:** Try to ping the client from the server. Check the IP address for the client. If you still have problems, talk to your network administrator.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 57

**Message:** client connection refused

**Explanation:** The client refused a connection on the port number for `bpcd`.

This error can occur because of the following:

- No process listening activity occurs on the `bpcd` port
- The number of connections to the `bpcd` port is more than the network subsystem can handle with the `listen()` call

**Recommended Action:** Do the following, as appropriate:

- For Windows NetBackup servers:
  - Make sure the NetBackup client software is installed.
  - Verify that the `bpcd` and `bprd` port numbers in the `%SystemRoot%\system32\drivers\etc\services` file on the server matches the setting on the client.
  - Verify that the **NetBackup Client Service Port** number and **NetBackup Request Service Port** number on the **Network** tab in the **NetBackup Client Properties** dialog match the `bpcd` and `bprd` settings in the `services` file. To display this dialog, start the Backup, Archive, and Restore interface on the server and click **NetBackup Client Properties** on the **File** menu. The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.
  - Verify that the NetBackup client service is running.
  - Use the following command to see if the master server returns correct information for the client:

```
install_path\VERITAS\NetBackup\bin\bpcIntcmd -pn
```

- On UNIX servers, do the following:
  - Make sure the NetBackup client software is installed.
  - Verify that the `bpcd` port number on the server (either NIS services map or in `/etc/services`) matches the number in the client's services file.
- Additional help is available.  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 58

**Message:** can't connect to client

**Explanation:** The server was unable to connect to the client.

**Recommended Action:** Resolve network communication problems.

See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 59

**Message:** access to the client was not allowed

**Explanation:** The master or the media server tries to access the client, but the client does not recognize the server as a valid server.

For the Enterprise Vault Agent: The names of all of the media servers among the Enterprise Vault servers are not specified in the client configuration.

**Recommended Action:** Do the following, as appropriate:

- If the server is a valid server, verify that it is in the server list on the client. If necessary add it as follows:
  - On Windows clients: Add the server on the **Server to use for backups and restores** drop-down in the **Specify NetBackup Machines and Policy Type** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click **Specify NetBackup Machines and Policy Type** on the **File** menu.

- On UNIX clients: Add a `SERVER` entry in the `bp.conf` file.  
 If you change the server list on a UNIX or Linux master server, do the following for the changes to take effect: Stop and then restart the NetBackup Request daemon (`bprd`) and NetBackup Database Manager daemon (`bpdgm`). On Windows, stop and restart the NetBackup Request Manager and NetBackup Database Manager services.
- On Windows clients, enable `bpinetd` debug logging as follows:
  - Create a `bpinetd` debug log directory on the client.
  - Increase the debug or log level.  
 See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
  - Retry the backup and examine the resulting logs to determine the cause of the failure.
- On all clients, enable `bpcd` debug logging as follows:
  - Create a `bpcd` debug log directory on the client.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.
  - Retry the backup and examine the resulting logs to determine the cause of the failure.
- Check the `bpcd` debug log to determine the server's peer name and what comparisons are made.  
 The `bpcd` process compares NetBackup server list entries to the peer name of the server that tries the connection. It rejects the connection if the names are different. If necessary, change the server list entry on the client to match the peer name.
- On Windows clients, check the following:
  - Verify that NetBackup for Windows software was installed under a Windows administrator account.  
 If NetBackup is under another type of account, reinstall it under an administrator account. The installation completes successfully under a non-administrator account except for the following: The NetBackup Client service is not added to Windows and the NetBackup server cannot access the client.
  - Verify that the Windows TCP/IP service specifies the domain server that resolves names for the subnet that contains the NetBackup servers.

UNIX, Linux, and Windows clients are frequently not on the same subnet and use different domain servers. When this condition exists, NetBackup servers and Windows clients may be able to ping one another, but the server still cannot access the Windows client.

- The preceding items may not resolve this problem.  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- If NetBackup use multiple network interfaces with media servers, make sure that the interface names appear in the client's `/usr/openv/netbackup/bp.conf` file.
- For the Enterprise Vault Agent: See the Troubleshooting section of the [NetBackup for Enterprise Vault Agent Administrator's Guide](#).
- Be sure that all name resolution services (primary, load-balancing, and secondary) are properly configured for consistent forward and reverse name resolution of NetBackup hosts.  
More information is available in the following technical article:  
<http://www.veritas.com/docs/TECH204794>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 60

**Message:** client cannot read the mount table

**Explanation:** The backup process on the client did not read the list of mounted file systems.

**Recommended Action:** Do the following, as appropriate:

- Run a `df` to see if the system can read the mount table.
- On an SCO system, code 60 can occur because the mount-point path name exceeds 31 characters (the maximum number on an SCO system). The `bpbkar` debug log on the client shows a message similar to the following:

```
bpbkar build_nfs_list: FTL - cannot statfs net Errno: 42406
```

To eliminate these errors for future backups, create a mount point with a shorter name and symbolically link the long name to the short name.

- For detailed troubleshooting information, create a `bpbkar` debug log directory. Then retry the operation and check the resulting log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 61

**Message:** the vneta proxy encountered an error

**Explanation:** The command or job was not able to perform secure communication operations. NetBackup may report additional information in a related code in the 76xx range of codes.

**Recommended Action:** Examine one of the following for a 76xx code that precedes the status code 61, and then look up the explanation for that 76xx code:

- Verbose or debug output from the command.
- The **Detailed Status** of the **Job Details** in the **NetBackup Administration Console**.
- The log file for the command or process that reported the status 61.

Click [here](#) to view technical notes and other information in the Veritas knowledge base about this status code.

## NetBackup status code: 63

**Message:** process was killed by a signal

**Explanation:** A kill signal was sent to the client process.

**Recommended Action:** The usual cause for this error is that someone intentionally terminated a backup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 64

**Message:** timed out waiting for the client backup to start

**Explanation:** The client did not send a ready message to the server within the allotted time.

**Recommended Action:** Do the following, as appropriate:

- On all clients, enable `bpcd` debug logging as follows:
  - Create a `bpcd` debug log directory on the client.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).

- On a UNIX, Linux, or Windows client, create the `bpbkar` debug log directory on the client.
- On Windows clients, verify that the NetBackup Client service is running.
- On a UNIX or Linux client, use the `ps` command to check for a client process that uses too much CPU time.
- Retry the backup and examine the debug logs for clues on the cause of the failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 65

**Message:** client timed out waiting for the continue message from the media manager

**Explanation:** The tape manager, `bptm`, reported that the media did not load and position within the allotted time.

**Recommended Action:** Verify that the requested volume is available and the required device is in an UP state.

- Create a `bptm` debug log directory on the server.
- On a UNIX or Linux NetBackup server, add the `VERBOSE` option to the `bp.conf` file. On a Windows NetBackup server, set the **Verbose logging level** option on the **Logging** tab in the **Master Server Properties** dialog box. See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
- Retry the operation and check the `bptm` debug log file for information on the drive, robot, and tape that causes the timeout.
- On a Windows NetBackup server (master or media): check the Event Viewer Application log for the error messages that indicate why the tape mount did not complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 66

**Message:** client backup failed to receive the CONTINUE BACKUP message

**Explanation:** The client `bpbkar` process did not receive the message from the server that indicates that the server is ready to continue.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
- On UNIX, Linux, and Windows clients, enable `bpbkcar` debug logging.
  - Create a `bpbkcar` debug log directory.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `bp.conf` file. On a Windows client, set **Verbose** on the **TroubleShooting** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then select **NetBackup Client Properties** from the **File** menu.
- On other PC clients, create a debug log directory for `bpcd`.  
Increase the amount of information that appears in the logs.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Use the `vxlogcfg` command as described in the following topic:  
See "About unified logging" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 67

**Message:** client backup failed to read the file list

**Explanation:** The client did not read the list of files to back up.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
- Set up debug logging.
  - On the server, create a `bpbrm` debug log directory.
  - On UNIX, Linux, and Windows clients, create a `bpbkcar` debug log directory.
  - On other PC clients, create a debug log directory for `bpcd`.  
Increase the amount of information that appears in the logs.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 68

**Message:** client timed out waiting for the file list

**Explanation:** The client did not receive the list of files to back up within the allotted time. This list comes from the server.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
  - Set up debug logging.
    - On the server, create a `bpbrm` debug log directory.
    - On UNIX, Linux, and Windows clients, create a `bpbkar` debug log directory.
    - On other PC clients, create a debug log directory for `bpcd`.
- Increase the amount of information that appears in the logs.  
 See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 69

**Message:** invalid filelist specification

**Explanation:** One of the following is true:

- VMware Intelligent Policy: Multiple backup components with the same *VM\_name* have conflicting information.
- The policy file list from the server has invalid entries.
- For the Enterprise Vault Agent: A policy contains some directives that cannot be specified together in the same policy.
- NetBackup Snapshot Client: In an off-host backup (**NetBackup Media Server** or **Third-Party Copy Device**), the file list contains the `ALL_LOCAL_DRIVES` entry. NetBackup does not support the `ALL_LOCAL_DRIVES` entry for off-host backups.

**Recommended Action:** Do the following, as appropriate:

- VMware Intelligent Policy: Check for duplication of the *VM\_name* of the VMs in the policy.

- Policy file list problem: Check the policy file list. If wildcards are used, verify that the bracket characters ([ and ]) in the list match. If the file list contains UNC (Universal Naming Convention) names, ensure that they are properly formatted. This error can occur if `nbjm` is running and a SharePoint job rediscovery returns a 0 or 1 and the policy file list is empty. Examine the `nbjm` unified log (originator ID 117) for more detail on the cause of the error.
- Enterprise Vault Agent: For more information, please see the Troubleshooting section of the *NetBackup for Enterprise Vault Agent Administrator's Guide* available from the following location:  
<http://www.veritas.com/docs/DOC5332>
- NetBackup Snapshot Client: Remove the ALL\_LOCAL\_DRIVES entry from the file list.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 70

**Message:** an entry in the filelist expanded to too many characters

**Explanation:** The wildcards, which were used in one of the file list entries, specified too many files.

**Recommended Action:** Change the wildcards in the file list to specify fewer files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 71

**Message:** none of the files in the file list exist

**Explanation:** The files in the file list did not match any of the files on the client. This error can occur with only one file in the file list and the file cannot be backed up due to an I/O error.

**Recommended Action:** Do the following, as appropriate:

- Verify that the correct file list is specified for this client.
- On Windows clients, verify that the account used to start the NetBackup Client service has read access to the files.  
 If you back up a network drive or a UNC (Universal Naming Convention) path, do the following: Use the Services application in the Windows Control Panel to verify that the NetBackup Client service does not start under the system account. The System Account cannot access network drives.

To back up network drives or UNC paths: Change the NetBackup Client service startup to log in as a user that has permission to access network drives.

- Check the All Log Entries report for clues.
- To set up debug logging, do one of the following:
  - On UNIX, Linux, and Windows clients, create a debug log directory for `bpbkar`.
  - On other PC clients, create a debug log directory for `bpcd`.
- Increase the amount of information that appears in the logs.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug logs.
- For an NDMP policy type, verify that the credentials of the NDMP hosts have been added. If not, add them.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 72

**Message:** the client type is incorrect in the configuration database

**Explanation:** The policy type attribute in the policy configuration indicates that the client is one type, but the installed software is for another type.

**Recommended Action:** Verify that the policy type attribute for the policy is correct.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 73

**Message:** `bpstart_notify` failed

**Explanation:** The `bpstart_notify` script returned a nonzero exit code.

**Recommended Action:** Check the `bpstart_notify` script on the client to see if it performs as expected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 74

**Message:** client timed out waiting for `bpstart_notify` to complete

**Explanation:** The `bpstart_notify` script on the client takes too long.

**Recommended Action:** Try to speed up the `bpstart_notify` script or set the `BPSTART_TIMEOUT` on the server to a value that is larger than the default. Set `BPSTART_TIMEOUT` in the `bp.conf` file on a UNIX or Linux NetBackup server. On a Windows NetBackup server, use Host Properties to set **Backup Start Notify Timeout**.

See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 75

**Message:** client timed out waiting for `bpend_notify` to complete

**Explanation:** The `bpend_notify` script on the client takes too long.

**Recommended Action:** Try to speed up the `bpend_notify` script or set `BPEND_TIMEOUT` on the server to a value that is larger than the default. Set `BPEND_TIMEOUT` in the `bp.conf` file on a UNIX or Linux NetBackup server. On a Windows NetBackup server, use Host Properties to set **Backup End Notify Timeout**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 76

**Message:** client timed out reading file

**Explanation:** A FIFO was specified in the file list and no data was produced on the FIFO within the allotted time.

**Recommended Action:** Make sure that the process that is to produce the data on the named FIFO is started correctly. Add an entry to the `/usr/openv/netbackup/bp.conf` file on the server to set `CLIENT_READ_TIMEOUT` to a larger value than the default.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 77

**Message:** execution of the specified system command returned a nonzero status

**Explanation:** An immediate command returned a nonzero status.

**Recommended Action:** Do the following, as appropriate:

- Verify that the command is specified correctly.
- For NetBackup Snapshot Client only, do the following:  
The policy file list may contain the files that do not reside within a file system that was designated as the snapshot source. To apply a snapshot method to the backup of individual files, the snapshot source must be a file system. (It cannot be a raw partition or Volume Manager volume.) The files in the policy file list must reside within that file system.
- Run the command manually to see if the wanted result is produced.
- For detailed troubleshooting information, set up debug logging as follows:
  - On UNIX, Linux, and Windows clients, create a debug log directory for `bpbkar`.
  - On other PC clients, create a debug log directory for `bpcd`.
  - Increase the amount of information that appears in the logs.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 78

**Message:** afs/dfs command failed

**Explanation:** Indicates an AFS `vos` command failure.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems Report for additional information on why the command failed.
- The `bpbkar` debug log shows the command that was run. Create a debug log directory for `bpbkar`. Retry the operation and retry the resulting debug log.
- Try running the `vos` command manually to duplicate the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 79

**Message:** unsupported image format for the requested database query

**Explanation:** One or more of the images to be synthesized was encrypted. These images cannot be synthesized.

**Recommended Action:** Ensure that none of the images were encrypted.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 80

**Message:** Media Manager device daemon (`ltid`) is not active

**Explanation:** If the server is UNIX or Linux, the NetBackup device manager daemon, `ltid`, is not running. If the server is Windows, the NetBackup Device Manager service is not running.

**Recommended Action:** Do the following, as appropriate:

- On Windows, use the Activity Monitor or the Services application in the Windows Control Panel to see if the NetBackup Device Manager service is running. If it is not running, start it. To enable verbose logging, place `VERBOSE` on a line by itself in the `install_path\Volmgr\vm.conf` file before you start the service.
- On UNIX, use `vmops` to see if `ltid` is running and if necessary start `ltid` in verbose mode with the following command:

```
/usr/opensv/volmgr/bin/ltid -v
```

Or, add a `VERBOSE` entry to the `/usr/opensv/volmgr/vm.conf` file. Create the `vm.conf` file if necessary.

- On UNIX, check the system logs to verify that `ltid` starts.

---

**Note:** On UNIX systems, `ltid`, and on Windows systems, the NetBackup Device Manager service, is used only if devices are attached to the system.

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 81

**Message:** Media Manager volume daemon (`vmd`) is not active

**Explanation:** The tape manager (`bptm`) did not communicate with the NetBackup Volume Manager (`vmd`). This communication is required for most operations.

**Recommended Action:** Do the following, as appropriate:

- On UNIX, verify that the Media Manager device daemon (`ltid`) and the NetBackup Volume Manager (`vmd`) are running. Start them if necessary.
- On Windows, verify that both the NetBackup Device Manager service and the NetBackup Volume Manager service are running. Start them if necessary.

---

**Note:** `ltid` or the NetBackup Device Manager service is used only if devices are attached to the system.

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 82

**Message:** media manager killed by signal

**Explanation:** Another process or a user terminated the tape manager (`bptm`) or disk manager (`bpdm`).

**Recommended Action:** This error should not occur in normal operation. If you want to terminate an active backup, use the NetBackup Activity Monitor.

When you back up a DomainOS client, this error occurs after the server has not received anything on the socket for at least 300 seconds. It causes a client read timeout and breaks the connection. The `bpbkar` debug log has an entry similar to the following:

```
13:22:49 [1347] <16> bpbkar: ERR - Extra output - - ECONNRESET
Connection reset by peer (UNIX/errno status)
```

To resolve the problem, increase the `CLIENT_READ_TIMEOUT` value. In this instance, set the value to 900.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 83

**Message:** media open error

**Explanation:** The tape manager (`bptm`) or disk manager (`bpdm`) did not open the device or file that the backup or restore must use.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report
- Event Viewer Application log (Windows)
- System log (UNIX)
- Typically, this status code indicates a drive configuration problem that allows more than one process at a time to open the device. On UNIX, the problem may be due one or more of the following:
  - Two (or more) devices were configured that are the same physical device (for different densities perhaps). Verify that none of the `/dev` files that were used for these devices have the same major or minor numbers.
  - Links exist in the file system that allows users access to the drives.
  - The configuration for the drives was modified (in the administrator interface or `vm.conf`) and the Media Manager device daemon, `ltid`, was not restarted. Verify the configuration and then start `ltid`.

On Windows, the problem may be that the Media and Device Management device configuration was modified but the NetBackup Device Manager service was not restarted. Verify the configuration and restart the NetBackup Device Manager service.

- On Windows, make sure that the tapes are not write protected.
- For detailed troubleshooting information:
  - Create a debug log directory for `bpdm` (if the device is disk) or `bptm` (if the device is tape).
  - On UNIX, restart `ltid` in the verbose mode by running the following:

```
/usr/opensv/volmgr/bin/ltid -v
```

Or, add a `VERBOSE` entry to the `/usr/opensv/volmgr/vm.conf` file. Create the `vm.conf` file if necessary.

- On Windows, to enable verbose logging, add `VERBOSE` on a line by itself in the `install_path\Volmgr\vm.conf` file. Then, stop and restart the NetBackup Device Manager service.
- Retry the operation and check the resulting debug log files.
- On Windows systems, look at the `install_path\VERITAS\NetBackup\db\media\errors` log for a drive that frequently produces errors.  
On UNIX systems, look at the `/usr/opensv/netbackup/db/media/errors` log (which is also included in the

`/usr/openv/netbackup/bin/goodies/support/support` script output) for a drive that frequently produces errors.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 84

**Message:** media write error

**Explanation:** The system's device driver returned an I/O error while NetBackup wrote to removable media or a disk file.

**Recommended Action:** Do the following, as appropriate:

- For NetBackup Snapshot Client only:  
If the following message appears in the `/usr/openv/netbackup/bptm` log, and the values for `key`, `asc`, and `ascq` are all zero (`0x0`) as shown in this example message:

```
tape error occurred on extended copy command, key = 0x0, asc =
0x0, ascq = 0x0
```

NetBackup Snapshot Client probably does not support your host-bus adapter and its driver. The host-bus adapters that are supported in the release are listed in the [NetBackup Release Notes](#).

- For additional information, check the following:
  - NetBackup Problems report to determine the device or media that caused the error
  - System and error logs for the system (UNIX)
  - Event Viewer Application and System logs (Windows)
- If NetBackup writes backups to a disk file, verify the following: The fragment size that is configured for the disk storage unit is not greater than the maximum file size that the operating system specifies.
- On Windows, make sure that the tapes are not write protected.
- If `bpbbackupdb` was used to back up the NetBackup catalog to a disk path on a UNIX or Linux system, the image you try to write may be greater than the maximum file size that is specified by that operating system. Tape files do not have this limit. You may have to back up the catalog to tape.
- If the media is tape, check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (refer to the `tpclean` command for robotic drives).

- The wrong media type. Verify that the media matches the drive type you use.
- Defective media. If it is defective, use the `bpmmedia` command to set the volume to the FROZEN state so it is not used for future backups.
- Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive.  
For example, on UNIX the drive may be configured for fixed mode when it must be variable mode.  
See the [NetBackup Device Configuration Guide](#) for more information.  
This configuration often results in the media being frozen with the message  

```
too many data blocks written, check tape and drive block size configuration
```

  
See "Frozen media troubleshooting considerations" in the [NetBackup Troubleshooting Guide](#).
- If you receive this error message when a GLACIER or LIFECYCLE backup job fails, the error is related to the Amazon lifecycle policy and occurs in the following situations:
  - The Amazon lifecycle policy that NetBackup uses cannot be applied. The Amazon GLACIER or LIFECYCLE storage class is not supported for the region to which the bucket belongs. Recreate the disk pool with the bucket in the supported region.
  - A different Amazon lifecycle policy other than what NetBackup uses already exists. Remove the policy that is not used by NetBackup and rerun the job.
  - The error occurred while creating the Amazon lifecycle policy that NetBackup uses to back up data to Amazon. Check the `bptm` logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 85

**Message:** media read error

**Explanation:** The system device driver returned an I/O error while NetBackup reads from tape or a disk file.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report to determine the device or media that caused the error
- System and error logs for the system (UNIX)

- Event Viewer Application and System logs (Windows)
- Check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
  - Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive.  
For example, on UNIX, the drive may be configured for fixed mode when it must be variable mode. More information is available.  
See the [NetBackup Device Configuration Guide](#).
  - Defective media. In this case, you may not be able to recover all the data on the media. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.  
See "Frozen media troubleshooting considerations" in the [NetBackup Troubleshooting Guide](#).
  - The wrong media type. Verify that the media matches the drive type you use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 86

**Message:** media position error

**Explanation:** The system's device driver returned an I/O error while NetBackup was positioning the tape media.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report to determine the device or media that caused the error
- System and error logs for the system (UNIX)
- Event Viewer Application and System logs (Windows)
- Check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
  - Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive.  
For example, on UNIX, the drive may be configured for fixed mode when it must be variable mode.

See the [NetBackup Device Configuration Guide](#) for more information.

- Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.  
See "Frozen media troubleshooting considerations" in the [NetBackup Troubleshooting Guide](#).
- The wrong media type. Verify that the media matches the drive type you use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 87

**Message:** media close error

**Explanation:** The system's device driver returned an I/O error while NetBackup closed a tape.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report to determine the device or media that caused the error
- System and error logs for the system (UNIX)
- Event Viewer Application and System logs (Windows)
- Check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
  - Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.  
See "Frozen media troubleshooting considerations" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 89

**Message:** problems encountered during setup of shared memory

**Explanation:** The NetBackup processes use shared memory for some operations. This status is returned when an error is encountered in the initialization of the shared memory by the operating system's APIs.

**Recommended Action:** Check for a shared memory problem. This error can occur if the system cannot allocate enough shared memory. It usually occurs with multiplexing, which increases the amount of shared memory that is required for the operation. An entry similar to the following may be seen in a NetBackup log or report:

```
system cannot allocate enough shared memory
```

If you see this type of message, refer to your platform vendor documentation for instructions on how to increase shared memory on your system.

For older levels of Solaris, you may need to change one or more default System V Shared Memory settings to prevent jobs failing with the memory allocation message, as follows:

- For Solaris 9, the default `shminfo_shmmax` value is 8 megabytes. You can place the following line in your `/etc/system` file to increase this setting. A value of 32 megabytes has been used in this example. Your system may require a greater value under some circumstances such as a high value for the NetBackup multiplexing parameter. According to Sun Microsystems documentation, setting this parameter to its maximum possible value has no side effects. (This parameter is not applicable to Solaris 10).

```
set shmsys:shminfo_shmmax=33554432
```

- For Solaris 9, the default `shminfo_shmmni` value is 100. You can place the following line in your `/etc/system` file to increase this setting. The default value is usually sufficient for NetBackup. In some circumstances, such as installing a NetBackup media server on a large database server, this setting may need to be increased. A value of 220 has been used in this example. (This parameter is not applicable to Solaris 10).

```
set shmsys:shminfo_shmmni=220
```

---

**Note:** If you modify any of these values in the `/etc/system` file, you must restart the system with `boot -r` for the new settings to take effect.

---

Refer to your vendor documentation for detailed instructions on how to modify these values. Note that these `shminfo` parameters are not applicable to Solaris 10.



Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 90

**Message:** media manager received no data for backup image

**Explanation:** The tape manager (`bptm`) or disk manager (`bpdm`) received no data when it performed a backup, archive, or duplication. This error can occur for incremental backups where no data was backed up because no files have changed.

**Recommended Action:** Do the following, as appropriate:

- Check the All Log Entries report.
- For detailed debug information, create `bpdm` or `bptm` debug log directories on the server. If the client is Windows, also create a `bpbkar` debug log directory on the client. Retry the operation and check the resulting debug logs.
- For additional information, check the following:
  - NetBackup Problems report to determine the device or media that caused the error
  - System and error logs for the system (UNIX)
  - Event Viewer Application log (Windows)
- Verify the Media and Device Management and system configuration for the drive.

For example, on UNIX, the drive may not be set for variable mode in a case where NetBackup requires that mode.

Check the [NetBackup Device Configuration Guide](#) for drive configuration information.
- Verify that the Media and Device Management configuration for the backup device matches what is specified for the storage unit in the NetBackup policy.
- Verify that you use the correct media in the drive.
- For detailed debug information, create a `bpdm` or `bptm` debug log directory (whichever applies) on the server. If the client is Windows, also create a `bpbkar` debug log directory on the client. Retry the operation and check the resulting debug logs.
- If the error occurred during duplication or a Vault session that uses an Alternate Read Server to perform duplication, verify that the Alternate Read Server has access to the source media.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 91

**Message:** fatal NB media database error

**Explanation:** The tape manager (`bptm`) received an error while it read or updated its media catalog.

**Recommended Action:** Do the following, as appropriate:

- Check the All Log Entries report for more information.
- Check the NetBackup Media Lists report to see if the catalog is intact. If the catalog is not intact, you may want to reload it from the latest NetBackup catalog backup volume.
- Verify that the disk partition on which the catalog resides has enough space.
- If these actions do not explain the problem, check the NetBackup Problems report.
- For detailed troubleshooting information, create a `bptm` debug log directory on the server and retry the operation. Check the resulting debug log file.
- Contact customer support and send appropriate problem and debug log sections.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 92

**Message:** media manager detected image that was not in tar format

**Explanation:** When you performed a restore, the tape manager (`bptm`) or disk manager (`bpdm`) did not find a `tar` header at the offset it expected.

**Recommended Action:** Do the following, as appropriate:

- Perform a `bpverify` of the affected image to determine if it is written correctly.
- Check the NetBackup Problems report for additional information about the error.
- Verify the Media and Device Management and system configuration for the drive.

For example, if you do not configure the drive for variable-mode block size writes on some UNIX systems, the backup images that write to the media produce this error when you attempt to restore the image.

The following sequence of events occurs:

- Backup succeeds.
- Verify succeeds.
- Restore fails.

The `bptm` debug log shows an error similar to the following:

```
00:58:54 [2304] <16> write_data: write of 32768 bytes indicated
only 29696 bytes were written, errno = 0
```

In this case, configure the drive for variable-mode block sizes and suspend the media that writes on that device.

See the [NetBackup Device Configuration Guide](#).

The images that were written to those media may be restorable (platform dependent), but single file restores are almost guaranteed to fail. You can expire these media and regenerate the backups. Or you can attempt to duplicate the images on these media to another device and then expire the original copy.

- This error has occurred on re-labeled and value-added 8-mm tape drives where the drive's micro code incorrectly processes a `forward space record` SCSI command.
- If the problem is not one of those discussed, create a debug log directory for either `bpdm` or `bptm` and retry the operation. Check the resulting debug log file.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 93

**Message:** media manager found wrong tape in drive

**Explanation:** When you load a volume for a backup or restore, the tape manager (`bptm`) found a volume that loaded without the expected tape header. This error may mean that volumes in a robot are not in the slots that are indicated in the Media and Device Management volume configuration.

**Recommended Action:** Do the following, as appropriate:

- If the volume is in a robot and the robot supports barcodes, perform a **Compare Contents with Volume Configuration** robot inventory (on Windows) or **Compare robot contents with volume configuration** robot inventory (UNIX). The resulting report shows the media ID that was found and validates its slot number with what is in the volume configuration. Then, either change the physical location in the robot or change the volume configuration to show the correct slot.

- If the volume was mounted on a nonrobotic drive, verify that the correct volume was mounted and assigned.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 94

**Message:** cannot position to correct image

**Explanation:** The tape manager (`bptm`) searched for a backup image to restore but did not find the correct backup ID at the expected position on the volume. This error can indicate a drive hardware problem.

**Recommended Action:** Do the following, as appropriate:

- Try the restore on another drive if possible.
- For additional information, check the following:
  - NetBackup Problems report to determine the device or volume that caused the error
  - System and error logs for the system (UNIX)
  - Event Viewer Application and System logs (Windows)
- For detailed troubleshooting information, create a debug log directory for `bptm` and retry the operation. Check the resulting debug log files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 95

**Message:** Media ID is not assigned to this host in the EMM database

**Explanation:** An operation was requested on a media ID for which NetBackup does not have a record assigned to the requesting server. For example, you use `bpmedia` to suspend or freeze a media ID that does not exist or is not assigned to the requesting server.

**Recommended Action:** Run a NetBackup Media List report to determine the valid media IDs and their assigned hosts. Then, retry the command with a valid media ID and assigned host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 96

**Message:** unable to allocate new media for backup, storage unit has none available

**Explanation:** The NetBackup Resource Broker (`nbrb`) did not allocate a new volume for backups. This error indicates that the storage unit has no more volumes available in the volume pool that is specified for this backup. Note that NetBackup does not change storage units during the backup.

**Recommended Action:** Check the NetBackup Problems report to determine the storage unit that is out of media.

- If the storage unit is a robot with empty slots, add more volumes (remember to specify the correct volume pool).
  - If there are no empty slots, move some media to nonrobotic and then add new volumes.
  - If you have difficulty keeping track of your available volumes, try the `available_media` script:  
On UNIX, this script is in:

```
/usr/openv/netbackup/bin/goodies/available_media
```

On Windows, the script is in:

```
install_path\NetBackup\bin\goodies\available_media.c  
d
```

This script lists all volumes in the volume configuration, and augments that list with information on the volumes currently assigned to NetBackup.

- Set up a scratch volume pool as a reserve of unassigned tapes. If NetBackup needs a new tape and none are available in the current volume pool, it does the following: Moves a tape from the scratch pool into the volume pool that the backup uses.
- If the storage unit and volume pool appear to have media, verify the following:
  - Volume is not FROZEN or SUSPENDED.  
Check for this condition by using the NetBackup Media List report. If the volume is frozen or suspended, use the `bpmedia` command to unfreeze or unsuspend it (if that is wanted).  
See "Frozen media troubleshooting considerations" in the [NetBackup Troubleshooting Guide](#).
  - Volume has not expired or exceeded its maximum number of mounts.
  - The EMM database host name for the device is correct.

If you change the EMM database host name, stop and restart the following:  
 The Media Manager device daemon, `ltid`, (if the server is UNIX or Linux)  
 or the NetBackup Device Manager service (if the server is a Windows system).

- The correct host is specified for the storage unit in the NetBackup configuration.  
 The host connection should be the server (master or media) with drives connected to it.
- The Media and Device Management volume configuration has media in the correct volume pool. Unassigned or active media is available at the required retention level.  
 Use the NetBackup Media List report to show the retention levels, volume pools, and status (active and so on) for all volumes. Use the NetBackup Media Summary report to check for active volumes at the correct retention levels.

- The NetBackup `bptm` process is rejected when it requests media from the `vmd` process (UNIX) or the NetBackup Volume Manager service (Windows). The cause of this problem is that the process or service cannot determine the name of the host that makes the request.

This error can be due to an incorrect network configuration that involves the following:

- Multiple network interfaces
- `/etc/resolv.conf` on those UNIX or Linux systems that use it
- Running DNS with reverse addressing not configured
- Create `bptm` and `vmd` debug log directories and retry the operation.
- Examine the `bptm` debug log to verify that `bptm` connects to the correct system. If an error is logged, examine the `vmd` log.

On UNIX, the `vmd` log is:

```
/usr/opensv/volmgr/debug/daemon/log.xxxxxx
```

On Windows, the `vmd` log is:

```
install_path\Volmgr\debug\daemon\xxxxxx.log
```

- If this storage unit is new and this attempt to use it is the first, stop and restart NetBackup on the master server.

---

**Note:** The mds unified logging files (OID 143) usually show the NetBackup media selection process.

---

More troubleshooting information in a wizard format is available for this status code.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 97

**Message:** requested media ID is in use, cannot process request

**Explanation:** An operation was requested on a media ID that is in use. An example of this operation is the attempt to suspend or freeze a volume while it is in use for a backup or restore.

**Recommended Action:** Retry the command when the volume is not in use. Use the Device Monitor to determine if the volume is in use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 98

**Message:** error requesting media (tpreq)

**Explanation:** The tape manager (bptm) received an error when it requested a media mount from the NetBackup Device Manager service (Windows) or the Media Manager device daemon (ltid) (UNIX).

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report to determine the reason for the failure. The most common cause is that the NetBackup Device Manager service (on Windows) or the Media Manager device daemon (ltid) (on UNIX) is not running. Start it if necessary.
- If you duplicate backups or use Vault to duplicate backups, this error could indicate the following: The Alternate Read Server does not have access to the tape where the original backup resides.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 99

**Message:** NDMP backup failure

**Explanation:** The paths in your NDMP policy file list did not back up successfully. One of the following occurred:

- None of the backup paths exist on the NDMP host.
- An NDMP backup uses a wildcard character that points to a file, not a file path.

**Recommended Action:** Do the following:

- Check the NetBackup All Log Entries report for more information.
- Try the following commands from another master server or media server:

```
# tpautoconf -verify ndmp_filer
# tpautoconf -probe ndmp_host
```

On the filer, verify that the NDMP service is running. The verification process depends on the filer.

For NetApp, run `ndmpd status` to verify that the NDMP daemon is running. If not, execute `ndmpd on` and re-run `ndmpd status` to verify.

- Change the NDMP wildcard to specify path names only. You cannot use a wildcard character that also matches a file name. For example, an NDMP backup selection is `/vol/vol_archive_01/autoit*`. This specification matches path name `/vol/vol_archive_01/autoit_01/`, but it also matches file name `/vol/vol_archive_01/autoit-v1-setup.exe`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 100

**Message:** system error occurred while processing user command

**Explanation:** A system call failure in `bparchive`, `bpbackup`, `bplist`, or `bprestore`.

**Recommended Action:** Do the following, as appropriate:

- Enable debug logging for `bparchive`, `bpbackup`, `bplist`, or `bprestore` (as appropriate) by creating debug log directories for them.  
On UNIX, if a nonroot user has problems, verify that the directory that was created has mode 666. Look for and correct any reported errors.
- Retry the operation and check the resulting logs.  
If the logs do not reveal the problem, use the command-line version of the command and correct any problems that are reported on `stderr`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 101

**Message:** failed opening mail pipe

**Explanation:** The process that attempts to send mail did not open the pipe to the server.

**Recommended Action:** Make sure that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` debug log directory and retry the operation. Check the resulting `bpcd` debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 102

**Message:** failed closing mail pipe

**Explanation:** The process that sends mail cannot close the pipe to the server.

**Recommended Action:** Make sure that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` debug log directory and retry the operation. Check the resulting `bpcd` debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 103

**Message:** error occurred during initialization, check configuration file

**Explanation:** NetBackup Snapshot Client can perform two kinds of off-host backups by means of a data mover: the NetBackup media server method or the Third-Party Copy Device method. For either method, an off-host data mover backup requires a configuration file (the `3pc.conf` file) to identify the following devices on the SAN:

- The client disks to back up
- The devices on which to store the data

If the media server has access to many disks and storage devices on the SAN, it may take too long to acquire the device information from the SAN. As a result, if no `3pc.conf` file exists on the media server, the first multistream backup that uses a data mover method may fail.

**Recommended Action:** Create the `3pc.conf` file manually before running the first multistream data mover backup. Use the following command to create the `3pc.conf` file:

```
# bptpcinfo -a
```

The `3pc.conf` file is created at `/usr/openv/volmgr/database/3pc.conf`.

More information is available on the `3pc.conf` file and how to create it.

See Configuring NetBackup for off-host data mover backups in the *NetBackup Snapshot Client Configuration* document available at the following location:

[https://www.veritas.com/content/support/en\\_US/article.TECH51377.html](https://www.veritas.com/content/support/en_US/article.TECH51377.html)

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 104

**Message:** invalid file pathname

**Explanation:** None

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 105

**Message:** file pathname exceeds the maximum length allowed

**Explanation:** The path name (built by using the current working directory) exceeds the maximum path length that the system allows.

**Recommended Action:** Shorten the current working directory path length.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 106

**Message:** invalid file pathname found, cannot process request

**Explanation:** One of the file paths to be backed up or archived is not valid.

**Recommended Action:** Do one or more of the following:

- Verify that the full path names are used and that they do not exceed the maximum path length for the system. (On UNIX, they start with a slash character [ / ].)
- Verify that the files exist and that the permissions allow NetBackup to access them.
- Some NDMP servers do not support directory-level expansion. Some NDMP filer vendors do not have the APIs that Veritas uses to support wildcard

characters lower than the volume level. For example, /fs1/dir\* is not a supported backup selection specification on EMC filers.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 108

**Message:** Action succeeded but auditing failed

**Explanation:** The primary action being audited has succeeded but the corresponding audit record has failed because it was never created.

For example, you use the `bppolicynew` command to create a policy and it returns status code 108. The policy is created successfully, but the associated audit record does not appear in the audit report that the `nbauditreport` command generates.

This error can be returned only if auditing is enabled using the `nbemmcmd` command.

**Recommended Action:** Do the following:

- Ensure that the `nbaudit` daemon (NetBackup Audit Manager) is running.
- Examine the logs responsible for the primary action and the `nbaudit` logs for more details on the cause of the error. For example, check the `bpdbm` logs for policy creation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 109

**Message:** invalid date specified

**Explanation:** This error can occur when you run a command on the command line that contains a date option. The format of a date option can vary depending on the locale of the master server.

**Recommended Action:** Do the following, as appropriate:

- If the error occurred on a command line, examine the standard error output from the command for an explanatory message.
- Refer to the format for the date options in the usage statement for the command. Look up the locale of the master server. Compare the date format of that locale with the date format on the usage statement for the command.
- Check the NetBackup Problems report for clues.

- If the error appears in a Java interface, enable the debug print manager in the Java startup file. Retry and compare the parameters that are logged in the Java log with the parameters listed in the command's usage statement.
- If these actions do not reveal the problem, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 110

**Message:** Cannot find the NetBackup configuration information

**Explanation:** On Windows, NetBackup did not read the registry entries that were created during installation. On UNIX, the `/usr/opensv/netbackup/bp.conf` file does not exist.

**Recommended Action:** On Windows, reinstall NetBackup software on the client. On UNIX, create a `/usr/opensv/netbackup/bp.conf` file with at least the following lines:

```
SERVER = server_name
CLIENT_NAME = client_name
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 111

**Message:** No entry was found in the server list

**Explanation:** On UNIX, the `SERVER = server_name` line is omitted from the `bp.conf` file. On Windows, the server list contains no entries.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX client, add the following line to the top of the `/usr/opensv/netbackup/bp.conf` file:

```
SERVER = server_name
```

- On a Microsoft Windows client, add the server name on the **Server to use for backups and restores** drop-down in the **Specify NetBackup Machines and Policy Type** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click **Specify NetBackup Machines and Policy Type** on the **File** menu.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 112

**Message:** no files specified in the file list

**Explanation:** A restore was requested with no files in the file list.

**Recommended Action:** Do the following, as appropriate:

- Specify at least one file to be restored.
- This status code may occur if `nbjm` is running and a stream discovery fails to find all stream files. Examine the `nbjm` unified log (originator ID 117) for more details on the cause of the error.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 114

**Message:** unimplemented error code

**Explanation:** This error should not occur. If `nbjm` received a negative error number, status 114 is issued.

**Recommended Action:** Examine the `nbjm` unified log (originator ID 117) for detailed information on the cause of the error.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 116

**Message:** VxSS authentication failed

**Explanation:** On either end of a socket connection, the parties did not mutually authenticate each other.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the Veritas Product Authentication Service is installed and configured. For complete installation instructions, see the *NetBackup Security and Encryption Guide* available from the following location:  
<http://www.veritas.com/docs/DOC5332>
- Check that both parties have a valid certificate. Examine the expiry date that is listed from a `bpnbat -WhoAmI`. For example:

```
bpnbat -WhoAmI
Name: JDOG
Domain: MYCOMPANY
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
Expiry Date: Sep 19 12:51:55 2009 GMT
Authentication method: Microsoft Windows
```

Operation completed successfully.

Shows an expiry date of September 19th, 2009. After 12:51:55 GMT this credential is no longer valid and a new credential is required.

- If you run from the NetBackup Administration Console, close and reopen the console. The console automatically obtains a credential for the currently logged in identity, if possible. By default, these certificates are valid for 24 hours. The following is an example of how to extend the credential beyond 24 hours to 30 days (2592000 seconds):

```
Windows: <install path>\veritas\netbackup\sec\at\bin\vssat
setexpiryintervals -p <plugin_name> -t <user> -e 2592000
```

```
UNIX: usr/opensv/netbackup/sec/at/bin/vssat setexpiryintervals -p
<plugin_name> -t <user> -e 2592000
```

- Ensure that the certificates for both sides use the same broker or are children of the same root broker and that trusts are established between them.  
See the [NetBackup Security and Encryption Guide](#) for more information on broker hierarchies and how to establish trust relationships between brokers.
- Ensure that connectivity between the physical systems in question is possible. If general sockets cannot connect between the computers (such as `ping` and `telnet`), issues within the network unrelated to NetBackup can cause this problem.
- Ensure that the system has sufficient swap space and the following directories are not full:
  - `/home/username`
  - `/usr/opensv/netbackup/logs`
  - `/tmp`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 117

**Message:** VxSS access denied

**Explanation:** The user identity that was used to attempt an operation does not have the permissions that are needed to perform the action.

**Recommended Action:** Do the following, as appropriate:

- If you use the default groups, make certain that the user attempts to perform an operation appropriate for that group. For example, a member of NBU\_Operators is unable to modify policy information, which is a permission reserved for administrator roles.
- Ensure that the system has sufficient swap space and the following directories are not full:
  - /home/username
  - /usr/openv/netbackup/logs
  - /tmp
- If you use your own defined groups and permissions, first determine the object with which the operation is associated. Then, add the permissions relative to the action. For example, a user is required to up and down drives but currently does not have permission to do so. Verify that the user belongs to the correct authorization group.

If necessary, verify that the group has Up and Down permissions on the Drive object within the **Group Permission** tab. If necessary, increase the verbosity level of NetBackup to locate what object and what permissions are required for the failing request. The pertinent lines in the debug logs look similar to the following:

```
17:19:27.653 [904.872] <2> GetAzinfo: Peer Cred Info.
Name: JMIZZLE
Domain: MYCOMPANY
Expiry: Sep 24 21:45:32 2003 GMT
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
AuthType: 1
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5082:
Function: VssAzAuthorize. Object
NBU_RES_Drives
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5083:
Function: VssAzAuthorize. Permissions Up
17:19:40.171 [904.872] <2> VssAzAuthorize: vss_az.cpp.5166:
Function: VssAzAuthorize. 20 Permission denied.
```

In this example, the user JMIZZLE attempts to perform an operation that requires the Up permission on the Drives object. To diagnose the problem, examine the

group(s) to which the user belongs to ensure that the appropriate group includes the Up permission. (Up is a member of the Operate permission set for Drives.)

- If you have performed disaster recovery and are now running catalog recovery using the **Remote Administration Console**, you need to restart the master server services. After the restart, if you do not logout from the **Remote Administration Console** and try to access the **Security Management** tab, you will receive this error message and must log in again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 118

**Message:** VxSS authorization failed

**Explanation:** NetBackup was unable to complete the authorization check against the authorization service.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the Veritas Product Authorization Service or daemon is running. See the [NetBackup Security and Encryption Guide](#) for more information on authentication and authorization daemons.
- Ensure that you are in communication with the correct master server. Within the `bp.conf` files on the local server, verify that the entry `AUTHORIZATION_SERVICES` specifies the proper host name (fully qualified) of the authorization service. For example, `AUTHORIZATION_SERVICE = machine2.mycompany.com 0` specifies that the server contacts machine2 to perform authorization checks. Also ensure that this entry matches that of the master server.
- Ensure that the system has sufficient swap space and the following directories are not full:
  - `/home/userName`
  - `/usr/opensv/netbackup/logs`
  - `/tmp`
- Ensure that the server that contacts the master has a valid certificate. The computer certificate can be examined as follows:

For UNIX:

```
# bpnbat -WhoAmI -cf
/usr/opensv/var/vxss/credentials/machine3.mycompany.com
```



### For Windows:

```
Bpnbat WhoAmI -cf "c:\Program
Files\VERITAS\NetBackup\var\vxss\credentials\machine3.my
company.com"
```

### Both of which would return:

```
Name: machine3.mycompany.com
Domain: NBU_Machines@machine2.mycompany.com
Issued by: /CN=broker/OU=root@machine2.mycompany.com/O=vx
Expiry Date: Sep  2 19:25:29 2004 GMT
Authentication method: Veritas Private Security
Operation completed successfully.
```

If the expiry date was exceeded, use `bpnbat -LoginMachine` to obtain a new credential for the computer.

See the [NetBackup Commands Reference Guide](#) for more information on `bpnbat`.

The server that attempts the check is not authorized to examine the authorization database. Ensure that `bpnbaz -ShowAuthorizers` re-tuned the computer's identity. Ensure that the computer has a computer credential under the directory as follows:

```
Program Files\VERITAS\var\vxss\credentials (Windows)
/usr/opensv/var/vxss/credentials (UNIX)
```

This credential should have the full name of the computer as in the following example: `machine1.company.com`.

- Check that the maximum number of open sockets to the authorization database was not exhausted. Use `netstat` to determine the number of sockets that are opened to port 4032 on the authorization server and that refer to the following configurations:

#### Windows:

```
HKLM\SOFTWARE\VERITAS\Security\Authorization\Communication\ClientMaxConnections
```

```
UNIX: /etc/vx/vss/VRTSaz.conf entryClientMaxConnections
```

If the maximum number of open connections was reached, you may need to increase the number of maximum open connections. An increase in the number of open connections increases the memory footprint of the authorization service or daemon. Note that extreme increases in the maximum number of connections can cause performance degradation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 120

**Message:** cannot find configuration database record for requested NB database backup

**Explanation:** The program that backs up the NetBackup internal catalogs did not find the attributes that indicate which media IDs to use or paths to back up. This error should not occur under normal circumstances.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.
- For detailed troubleshooting information, create `admin` and `bpdbm` debug log directories and retry the operation. Check the resulting debug logs.
- Contact customer support and send the appropriate problem and debug log sections that detail the error.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 121

**Message:** no media is defined for the requested NB database backup

**Explanation:** When NetBackup attempted to back up its internal catalogs, no media IDs were defined in the catalog backup configuration.

**Recommended Action:** Add the media IDs to the catalog backup configuration. Verify that the media IDs are in the NetBackup volume pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 122

**Message:** specified device path does not exist

**Explanation:** The NetBackup internal catalogs were backed up by using the `bpbackupdb` command line and by specifying a device path (on Windows) or a raw device file (on UNIX) that does not exist.

**Recommended Action:** Retry the command by using a valid device file name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 123

**Message:** specified disk path is not a directory

**Explanation:** When NetBackup attempted to back up its internal catalogs, the backup attributes were set to dump to a disk. However, the disk file path already exists and is not a directory.

**Recommended Action:** Specify a different disk path for the catalog backup or delete the file that already exists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 124

**Message:** NB database backup failed, a path was not found or is inaccessible

**Explanation:** One or more of the specified paths in the catalog backup configuration are not backed up.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.  
The following are some possible causes:
  - The path does not exist.
  - On a UNIX system, one of the paths contains a symbolic link.
- After you determine which path cannot be accessed, correct the path names in the catalog backup configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 125

**Message:** a NetBackup catalog backup is in progress

**Explanation:** Only one NetBackup catalog backup can be active at any given time. Certain operations are not allowed during an online catalog backup. (These include catalog archiving, catalog compression, and expiration of the last copy of an image.)

**Recommended Action:** Retry the operation after the catalog backup completes.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 126

**Message:** NB database backup header is too large, too many paths specified

**Explanation:** Too many paths were specified in the NetBackup catalog backup configuration to fit in a fixed-size media header. This error should not occur under normal circumstances.

**Recommended Action:** Delete some of the paths from the catalog backup configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 127

**Message:** specified media or path does not contain a valid NB database backup header

**Explanation:** The `bprecover` command was issued and the media ID specified does not have valid catalog backup data.

**Recommended Action:** Validate that the correct media ID is used.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 128

**Message:** NB database recovery failed, a process has encountered an exceptional condition

**Explanation:** In the catalogs that were specified for recovery, one or more cannot be restored. For more detail, refer to the error message that precedes this status code in the output from the `bprecover` command.

**Recommended Action:** Do the following, as appropriate:

- Fix the problem that was reported in the error message in the `bprecover` output.
- Identify which NetBackup services to shut down before a NetBackup database recovery attempt:  
 See "About recovering the NetBackup catalog" in the [NetBackup Troubleshooting Guide](#).  
 The NetBackup services should be shut down except for the NetBackup Client Service, which must be running for the database recovery to succeed.
- Check the NetBackup Problems report for additional information about the error.  
 The following are some possible causes:

- A disk may be full.
- The NetBackup catalog tape may be corrupt.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 129

**Message:** Disk storage unit is full

**Explanation:** As NetBackup writes to the file system for the disk storage unit, runs out of space. Until more file system space is available, images of similar size or larger may fail with this error when written to this disk storage unit.

In a scheduled backup job that writes to a storage unit group (which contains this disk storage unit), the following occurs: the NetBackup scheduler requests the storage unit with the greatest available capacity when the job is retried.

For the retry, when the scheduler requests the storage unit with the greatest available capacity, note the following:

- A tape storage unit in the storage unit group has preference over any disk storage units since tape storage units usually have more capacity.
- If the storage unit with the most unused capacity is busy, NetBackup skips it. NetBackup then selects an available storage unit with the next largest, unused capacity.
- If the storage unit with the greatest unused capacity is the one that lacked capacity when the job first failed, the scheduler tries it again. That storage unit may have more unused capacity now than it did when the job failed.

**Recommended Action:** Do the following, as appropriate:

- Either free sufficient space or add more space to the file system for this storage unit.
- Lower the high capacity mark for this disk storage unit. Configure the policies to access it through a storage unit group that provides alternative storage to use when this storage unit fills up. Ideally, if an image exceeds the file system's high capacity mark, it also completes successfully. This image leaves the storage unit in a full state (over the high capacity mark). The storage unit then is not assigned to other jobs until its capacity falls under its high capacity mark.
- If the Staging attribute is set on the disk storage unit that did not have enough capacity, it may be unable to create free space. It cannot create space because the backups that are staged to the disk are not relocated (eligible to be deleted from the staging storage unit). Ensure that staging's relocation (duplication) jobs

successfully copy enough images to provide sufficient free space for new backups.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 130

**Message:** system error occurred

**Explanation:** An error occurred that prevents the product from operating in a consistent fashion. This error is usually related to a system call.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.
- Check the system log for reported problems.
- For detailed troubleshooting information, create `bpdbm`, `bptm`, and `bprd` debug log directories on the master server. Increase the unified logging level by using the `vxlogcfg` command.

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

- Retry the operation and check the resulting debug logs.

If the policy validation fails, it is due to one of following reasons:

- There is a certificate mismatch on the client. Remove the CloudPoint CA certificate from the following location and validate the policy again:

`install_location/var/global/cloudpoint_certificates`

- The CloudPoint server is not accessible.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 131

**Message:** client is not validated to use the server

**Explanation:** The client name, as determined from the connection to the server, did not match any client name in the NetBackup configuration. No `altnames` configuration for this client exists on the master server. A client and server with multiple network connections can encounter this problem in the following situation: the name by which the client is configured is not the one by which its routing tables direct connections to the server.

**Recommended Action:** Do the following, as appropriate:

- Examine the NetBackup Problems report.

- Create a debug log directory for `bprd` and retry the operation. Check the resulting debug log to determine the connection and the client names.

Depending on the request type (restore, backup, and so on), you may need or want to do the following:

- Change the client's configured name.
- Modify the routing tables on the client.
- On the master server, set up an `altnames` directory and file for this client. See the [NetBackup Administrator's Guide, Volume I](#).  
Or
- On a UNIX master server, create a soft link in the NetBackup image catalog.
- See Verifying host names and services entries in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 132

**Message:** user is not validated to use the server from this client

**Explanation:** None

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 133

**Message:** invalid request

**Explanation:** One of the following has occurred:

- You make an unrecognizable request. This lack of recognition usually results from different versions of NetBackup software being used together.
- A client receives this error in response to a list or restore request. The `DISALLOW_CLIENT_LIST_RESTORE` or `DISALLOW_CLIENT_RESTORE` option exists in the `bp.conf` file on a UNIX NetBackup server or in the registry on a Windows NetBackup server. These options deny list and restore requests from all NetBackup clients.

**Recommended Action:** Do the following, as appropriate:

- If you suspect that the software versions are the problem, verify that all NetBackup software is at the same version level.
  - On UNIX NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
  - On Windows NetBackup servers, check the `install_path\netbackup\version.txt` file or the **About NetBackup** item on the **Help** menu.
  - On Microsoft Windows clients, check the **About NetBackup** item on the **Help** menu.
- If the server denies list and restore requests, do one of the following:
  - Go to the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers**. In the right pane, double-click the master server you want to modify. In the properties dialog box, in the left pane, select **Client Attributes** to access the **Allow client browse** and **Allow client restore** options.
  - Remove the `DISALLOW_CLIENT_LIST_RESTORE` and `DISALLOW_CLIENT_RESTORE` options from the `bp.conf` file on a UNIX NetBackup server or from the registry on a Windows NetBackup server. Then, stop and restart the NetBackup request daemon (UNIX) or NetBackup Request Manager service (Windows).
- For detailed troubleshooting information, create `bpdbm`, `bprd`, and `admin` debug log directories. Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 134

**Message:** unable to process request because the server resources are busy

**Explanation:** Status code 134 is an informational message that indicates that all drives in the storage unit are currently in use. If all drives are in use, NetBackup automatically tries another storage unit. If one is not available, NetBackup re-queues the job with a status of 134 and retries it later.

**Recommended Action:** None

The 134 code is an informational message only and is not considered an error. It can occur for a number of reasons in normal operation. The 134 status code can occur more frequently in an SSO environment. No action is necessary.



A status 134 is not logged in the error logs. A 134 status causes a new try to appear in the Activity Monitor. It does not increase the retry count that is associated with the allowed number of retries.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 135

**Message:** client is not validated to perform the requested operation

**Explanation:** An alternate client restore was tried that does not come from the root user (on UNIX) or the administrator (on Windows).

**Recommended Action:** Retry the operation as a root user (on UNIX) or as an administrator (on Windows) on the master server. Also see status code 131.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 136

**Message:** tir info was pruned from the image file

**Explanation:** The TIR information was pruned from one or more of the component (differential or cumulative) backup images being synthesized.

This situation arises when the following occurs:

- The most recent backup image for the client is a synthetic full or cumulative backup
- The TIR information from one or more of the component images before the synthetic full (or cumulative) backup is pruned

The TIR information is automatically restored to the image catalog if you expire the synthetic backup (full or cumulative) image and try to rerun the synthetic backup job for the client. However, the synthetic backup job fails with this error if the TIR restore fails due to bad, missing, or vaulted media or a bad drive.

**Recommended Action:** Reimport the TIR information into the catalog of each component image (from which the TIR information was pruned). Then rerun the synthetic backup job. The TIR information can be imported into the image catalog by initiating a true image restore of any file from that component image. The restore process also restores the TIR information in the image catalog.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 140

**Message:** User ID was not superuser

**Explanation:** A user or process that did not have root privileges (on UNIX) or administrator privileges (on Windows) started the process.

**Recommended Action:** If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX) and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 141

**Message:** file path specified is not absolute

**Explanation:** The file specification must be an absolute path.

**Recommended Action:** Correct the file specification and retry the command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 142

**Message:** file does not exist

**Explanation:** To back up a VxFS file system with Snapshot Client, the VxFS file system on the client must be patched with correct, dynamically linked libraries. If the correct VxFS libraries are not installed, the backup fails with status 142.

The following appears in the log:

- For most snapshot backups, the following message appears in the `/usr/openv/netbackup/logs/bpfis` log on the client:

```
09:36:48.299 [527] <32> fs_dev_rt_check: FTL - snapshot method:
nbu_snap abort - required VxFS dynamic linked libraries for
NetBackup are not installed. Please visit the Veritas support
website, and refer to Technote number 262225 for further
information.
```

- For the backups that run from a FlashBackup policy, the following appears in the `/usr/openv/netbackup/logs/bpbkar` log on the client:

```
10:09:56.566 [1146] <32> bpfsmmap: FTL - bpfsmmap: FlashBackup
abort - required VxFS dynamic linked libraries for NetBackup are
not installed. Please visit the Veritas support website, and
```

```
refer to Technote number 262225 for further information.
10:09:56.571 [1146] <16> bpbkar Exit: ERR - bpbkar FATAL exit
status = 142: file does not exist
10:09:56.573 [1146] <4> bpbkar Exit: INF - EXIT STATUS 142: file
does not exist
```

- The `bpexpdate`, `bpimmedia`, `bpimport`, and `bpverify` commands return this status code if you cannot gather disk pool, disk volume, disk pool volume, disk media IDs, or server type information.
- The `bpbkar` returns this status code if a checkpoint clone is missing, or if a frozen image backup does not return the snapshot information.

**Recommended Action:** Install the VxFS dynamic libraries on the NetBackup client as described in tech note TECH28008 and try the backup again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 143

**Message:** invalid command protocol

**Explanation:** A poorly formed request was made to the NetBackup request daemon (UNIX) or to the Request Manager service (Windows). This error can be due to the following: mismatched versions of the product, corrupted network communication, or to a non-NetBackup process sending data across the port for the daemon or service.

**Recommended Action:** Examine the NetBackup error logs to determine the system that was the source of the data. On that system, determine the process that initiated the request. If it was a NetBackup process, verify that the process or command is compatible with the version of software on the server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 144

**Message:** invalid command usage

**Explanation:** This status code is due to a NetBackup process being started with improper options or an incompatibility in the product.

**Recommended Action:** Either correct the command or verify that all NetBackup binaries are at the same version level.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 145

**Message:** daemon is already running

**Explanation:** Another copy of the process is running.

**Recommended Action:** Terminate the current copy of the process and then restart the process.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 146

**Message:** cannot get a bound socket

**Explanation:** The service or daemon did not bind to its socket. A system call fails when the daemon (UNIX) or service (Windows) attempts to bind to its configured port number. This error is usually caused when another process acquired the port before the daemon or service started.

**Recommended Action:** Do the following, as appropriate:

- Examine the NetBackup Problems and All Log Entries reports.
- Create `bprd` and `bpbm` debug log directories and retry the operation. Check the resulting logs to see the system error message that resulted from the attempt. If another process has the port, use other system commands to determine the process. Based on this research, either change the port number in your `services` file or map or terminate the process that acquired the port.

On UNIX, another possible cause for this error is the use of the `kill` command to terminate `bprd` or `bpbm`. To stop `bpbm`, use the

`/usr/openv/netbackup/bin/bpbm -terminate` command. Use of the `kill` command to stop these processes can leave them unable to bind to their assigned ports the next time they are started.

To identify a `bprd` or a `bpbm` problem, look for lines similar to the following in the debug log for the respective process:

```
<16> getsockbound: bind() failed, Address already in use (114)
<32> listen_loop: cannot get bound socket. errno = 114
<4> terminate: termination begun...error code = 146
```

Similar entries can appear in the reports.

- If the problem persists longer than 10 minutes, it may be necessary to restart the server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 147

**Message:** required or specified copy was not found

**Explanation:** The requested copy number of a backup or an archive image cannot be found.

**Recommended Action:** Correct the request to specify a copy number that does exist.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 148

**Message:** daemon fork failed

**Explanation:** A NetBackup service did not create a child process due to an error that was received from the system. This error is probably an intermittent error that is based on the availability of resources on the system.

**Recommended Action:** Do the following, as appropriate:

- Restart the service at a later time and investigate the system problems that limit the number of processes.
- On Windows systems, check the Event Viewer Application and System logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 149

**Message:** master server request failed

**Explanation:** None

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 150

**Message:** termination requested by administrator

**Explanation:** Using the GUI, an administrator terminates an active process. The job status changes to FAILED.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 152

**Message:** required value not set

**Explanation:** An incomplete request was made to the `bpdbm` process (on UNIX), or the NetBackup Database Manager service (on Windows). This error usually occurs because different versions of software are used together.

**Recommended Action:** Do the following, as appropriate:

- Verify that all software is at the same version level.
- For detailed troubleshooting information, create `bpdbm` and `admin` debug log directories and retry the operation. Check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 153

**Message:** server is not the master server

**Explanation:** This status code is reserved for future use.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 154

**Message:** storage unit characteristics mismatched to request

**Explanation:** A backup was tried and the storage unit selected for use had the characteristics that were not compatible with the backup type.

**Recommended Action:** Verify that the characteristics of the selected storage unit are appropriate for the attempted backup.

- For a NetBackup Snapshot Client, the policy storage unit was set to **Any\_available** and the off-host backup method was set to **Third-Party Copy Device** or **NetBackup Media Server**. Do not choose **Any\_available**. A particular storage unit (such as `nut-4mm-robot-t14-0`) must be specified when **Third-Party Copy Device** or **NetBackup Media Server** is specified as the off-host backup method.
- For an NDMP policy type, verify the following:
  - You have defined a storage unit of type NDMP.
  - The NDMP host value matches the host name of the client. For example, if the NDMP policy specifies `toaster` as the client, the configuration for the storage unit must specify `toaster` as the NDMP host.
  - The media server for the storage unit is running the correct version of NetBackup.
- For a policy type other than NDMP, verify that the policy specifies a media manager or disk type storage unit.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 155

**Message:** disk is full

**Explanation:** The write to the catalog file failed because the disk that contains the catalog database is full, or the track log folder is full.

**Recommended Action:** Free up space on the disks where NetBackup catalogs reside or where the track log folder resides and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 156

**Message:** snapshot error encountered

**Explanation:** The following are possible causes of this status code:

- Errors related to VMware
- An error related to the Enterprise Vault Agent. The following errors can result in a status code 156:
  - VSS\_E\_BAD\_STATE snapshot error
  - VSS\_E\_INSUFFICIENT\_STORAGE snapshot error

- A snapshot-backup related error regarding Windows Open File Backup or Snapshot Client.
- Multiple volumes are mounted to the same mount point

**Recommended Action:** Do the following, as appropriate:

- **For NetBackup for VMware:**

- NetBackup cannot obtain the volume ID of a drive  
 NetBackup may not be able to obtain the volume ID of a drive. In that case, none of the virtual machine drives are backed up. The backup fails with NetBackup status code 156.  
 The drive may be down.

- A backup of the virtual machine is already active  
 You cannot run more than one backup per virtual machine at a time. If you start a second backup of the virtual machine while the first backup is active, the second job fails with a status 156.  
 Recommended action: Wait until the first job completes, then run the second one.

- Cannot find virtual machine name  
 NetBackup cannot find the host name or VM display name of a virtual machine that is listed in the backup policy. The detailed status log may include the following error message:

```
Critical bpbrm (pid=<pid number>) from client <client name>:  
FTL - snapshot creation failed, status 156.)
```

If the virtual machines do not have static IP addresses, you can configure NetBackup to identify virtual machines by their VM display names or UUIDs. Examples of the environments that do not use static IP addresses are clusters, and the networks that assign IP addresses dynamically.

Note that NetBackup may have been configured to identify virtual machines by their VM display names. In that case, make sure that the display names are unique and that they do not contain special characters.

- The virtual machine is turned off  
 Through a vCenter server, NetBackup can back up the virtual machines that are turned off. You must provide credentials for NetBackup to access the vCenter server.

If NetBackup uses credentials for an ESX server instead of vCenter, it may not be able to identify a turned off virtual machine. Note the following:

- If the policy uses VM host name or VM DNS name as the Primary VM identifier, NetBackup may not find the virtual machine. The backup fails.



- If the policy uses VM display name or VM UUID as the Primary VM identifier, NetBackup can identify the virtual machine. The backup succeeds.
- The virtual machine has one or more independent disks and is in a suspended state

If a virtual machine with independent disks is in a suspended state, snapshot jobs fail. Messages similar to the following appear in the job details log:

```
01/12/2015 17:11:37 - Critical bpbrm (pid=10144) from client
<client name>: FTL - VMware error received: Cannot take a
memory snapshot, since the virtual machine is configured with
independent disks.
```

More information is available in the following VMware article:

<http://kb.vmware.com/kb/1007532>

As a workaround, change the state of the virtual machine to on or off, and rerun the backup.

---

**Note:** Data on independent disks cannot be captured with a snapshot. The rest of the virtual machine data is backed up.

---

- The virtual machine's disk is in raw mode (RDM)  
The RDM is ignored (not backed up) and any independent disk is recreated but empty.
- The attempt to create a snapshot exceeded the VMware timeout  
If the attempt to create a snapshot of the virtual machine exceeds the VMware timeout of 10 seconds, the snapshot fails with NetBackup status 156. This timeout may occur if the virtual machine is configured with a large number of volumes. Note that the timeout may be encountered even if the **Virtual machine quiesce** option was disabled.

Do one of the following:

- Reduce the number of volumes within the virtual machine.
- Install a NetBackup client on the virtual machine and select another backup method for the policy (not the VMware snapshot method).
- The virtual machine has no vmdk file assigned  
Virtual machines without vmdk files can occur in a vCenter Site Recovery Manager (SRM) environment. If a replicated virtual machine has never been active, it is in passive mode and may have no vmdk file(s).

You can enable the **Ignore diskless VMs** option on the **VMware Advanced Attributes** tab of the policy. If this option is enabled: NetBackup does not back up a replicated (passive) virtual machine in an SRM environment if that virtual machine has no vmdk files.

- The vmdk file has too many delta files  
Whenever a VMware snapshot occurs, a delta.vmdk file is created for each vmdk. If 32 or more such delta files exist for a single vmdk file, a NetBackup backup of that VM may fail (status 156). The NetBackup Activity Monitor job details contain messages similar to the following:

```
02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from
client fl5vml_2012: FTL - vSphere_freeze: Unable to proceed with
snapshot creation, too many existing delta files(44).
02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from client
fl5vml_2012: FTL - VMware_freeze: VIXAPI freeze (VMware snapshot)
failed with 25: SYM_VMC_FAILED_TO_CREATE_SNAPSHOT
02/06/2015 10:33:17 - Critical bpbrm (pid=15799) from client
fl5vml_2012: FTL - vfm_freeze: method: VMware_v2, type: FIM,
function: VMware_v2_freeze
```

To back up the VM, do the following:

- Consolidate the VM's snapshots.  
In the VMware interface, right-click on the VM and select **Snapshot > Consolidate**. For more information, see your VMware documentation.
- Verify that each of the VM's vmdk files now has fewer than 32 delta files.  
If the snapshot consolidation was not successful, see the following VMware article for further assistance:  
<http://kb.vmware.com/kb/1004545>
- Rerun the NetBackup backup.
- VMware snapshot quiesce operation failed  
If the NetBackup policy is enabled for virtual machine quiesce (the default), the VMware snapshot operation in vSphere initiates a quiesce of the virtual machine. If snapshot quiesce fails, the NetBackup job fails with status 156.
- **For the Enterprise Vault Agent:**  
See the Troubleshooting section of the [NetBackup for Enterprise Vault Agent Administrator's Guide](#).
- **For a Windows Open File Backup Snapshot Provider that uses VSS:**  
See the Troubleshooting section of one of the following guides:
  - [NetBackup for VMware Administrator's Guide](#)

- [NetBackup for Hyper-V Administrator's Guide](#)
- [NetBackup Snapshot Client Administrator's Guide](#)

The VSS cache files may be too small for the number of files being backed up using VSS.

If `bpbkar` debug logs are turned on, a message similar to the following appears in the `bpbkar` debug log for the backup.

```
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -
failure reading file: D:\ test.file (WIN32 5: Access is denied.
)
8:51:14.569 AM: [1924.2304] <4> tar_base::V_vTarMsgW: INF - tar
message received from dos_backup::tfs_readdata
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -
Snapshot Error while reading test.file
8:51:14.569 AM: [1924.2304] <4> tar_base::V_vTarMsgW: INF - tar
message received from tar_backup::nextfile_state_switch
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: FTL -
Backup operation aborted!
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: INF -
Client completed sending data for backup
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: INF - EXIT
STATUS 156: snapshot error encountered
```

To increase the VSS cache size by using the Shadow Copy configuration in Windows, do the following in the order listed:

- In Windows, right-click **My Computer** and select **Manage**.
- In the console tree, right-click **Shared Folders**, select **All Tasks**, and select **Configure Shadow Copies**.
- Select the volume where you want to make changes, and then select **Settings**.
- In the **Settings** dialog box, change the **Maximum Size** setting to either of the following: No Limit or a size large enough to suit the requirements of your installation and your usage of VSS.
- **For backups using Snapshot Client and the NAS\_Snapshot method, with or without SnapVault:**
  - If the backup fails with status code 156, consult the `bpfis` legacy log, in `/usr/opensv/netbackup/logs` (UNIX) or `install_path\NetBackup\logs` (Windows). If the `bpfis` directory does not already exist, you must create it and rerun the job.
  - If necessary, increase the logging level and retry the job.

See "About logs" in the [NetBackup Logging Reference Guide](#).

- On Windows clients, when restoring files from a backup that is made with the NAS\_Snapshot method, log into the NetBackup Client Service as the Administrator account, not as the local system account. Otherwise, the backup fails with status 156.
  - In Windows Services, double-click the NetBackup Client Service.
  - Then check the **Log On** tab: if the service is not logged on as Administrator, stop the service.
  - Change the logon to the Administrator account and restart the service.
  - Retry the restore.
- For other NetBackup Snapshot Client issues:
  - The file system that is specified as a snapshot source is not mounted. In this case, you may see the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
17:12:51 bpfis: FTL - snapshot creation failed, status 156
17:12:51 bpfis: INF - EXIT STATUS 156: snapshot error
encountered
```

And the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_vfms_logf: INF - cannot snap_on, err: 5
17:12:51 delete_mount_point: INF - Deleted mount point
/tmp/___jody_test:20958
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following
messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - vfm_freeze: method: nbu_snap, type:
FIM, function: nbu_snap_freeze
17:12:51 onlfi_freeze: FTL - VfMS method error 5; see following
message:
17:12:51 onlfi_freeze: FTL - nbu_snap_freeze: Cannot turn on
snapshot; snapshot source=/opt, cache=/dev/rdisk/clt3d1s0, snap
error=5
17:12:51 onlfi_thaw: WRN - / is not frozen
```

Make sure that the file system that is specified for the snapshot source has been mounted.

- The file system that is specified as the snapshot source does not correspond to the file system that contains the actual files (as opposed to symbolic links to the files). The mounted file system for the snapshot source must contain

the actual files, not symbolic links. If items in the file list, such as `/oracle`, is a symbolic link to `/export/home/oracle`, the snapshot source must specify `/export`, or `/export/home`, not `/oracle`.

- **VxVM** is selected as the snapshot method but the snapshot source is not configured over a Veritas Volume Manager (VxVM) volume. In this case, you may see the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
17:12:51 bpfis: FTL - snapshot creation failed, status 156
17:12:51 bpfis: INF - EXIT STATUS 156: snapshot error
encountered
```

And something like the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_vfms_logf: INF - vxvm_freeze: Snapshot source
/cockpit1 on device /dev/dsk/clt0d0s6 is not on a VxVM volume
17:12:51 delete_mount_point: INF - Deleted mount point
/tmp/_cockpit1_coc_group1:3518
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following
messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
17:12:51 onlfi_freeze: FTL - VfMS method error 9; see following
message:
17:12:51 onlfi_freeze: FTL - vxvm_freeze: Snapshot source
/cockpit1 on device /dev/dsk/clt0d0s6 is not on a VxVM volume
17:12:51 onlfi_thaw: INF - fim=vxvm
17:12:51 onlfi_thaw: WRN - /cockpit1 is not frozen
```

Make sure that the snapshot source is configured over a Veritas Volume Manager (VxVM) volume.

- **VxVM** was selected as the snapshot method, but a Veritas Volume Manager snapshot mirror of the snapshot source volume had not been created before you ran the backup, or another backup is currently running that uses the snapshot mirror. In either case, you may see the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following
messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
17:12:51 onlfi_freeze: FTL - VfMS method error 3; see following
```

```
message:
17:12:51 onlfi_freeze: FTL - find_ready_snapshot: Cannot find
available snapshot mirror
```

See the [NetBackup Snapshot Client Administrator's Guide](#) for information on how to create a snapshot mirror on the client before you run the backup.

- **VxVM** was selected as the snapshot method, and a Veritas Volume Manager snapshot mirror of the snapshot source volume has been created. However, two different backup jobs (A and B) try to back up the same volume (for example, `vol101`), but job A starts before job B. After an available snapshot mirror is found, a brief pause occurs before the snapshot is formed. Job B that runs slightly behind job A may try to create a snapshot of the snapshot mirror immediately before job A creates the snapshot and gets the lock on it.

In this case, you may see the following in the

`/usr/openv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following
messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
17:12:51 onlfi_freeze: FTL - VfMS method error 3; see following
message:
17:12:51 onlfi_freeze: FTL - vxvm_freeze: Command failed with
status=11: /usr/sbin/vxassist -g rootdg snapshot vol101
VfMSCAAu7a4Uw </dev/null>/var/tmp/VfMSAAAs7a4Uw
2>/var/tmp/VfMSBAAt7a4Uw
```

The job that was unable to get a lock (job B in the preceding example) fails, and must be run again.

- When you use `nbu_snap` as a snapshot method, you may have stale snapshots if status code 156 occurs with the following messages in the `/usr/openv/netbackup/logs/bpfis` log. (Stale snapshots are those that `nbu_snap` did not automatically delete.)

```
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following
messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - vfm_freeze: method: nbu_snap, type:
FIM, function: nbu_snap_freeze
17:12:51 onlfi_freeze: FTL - VfMS method error 5; see following
```

```
message:
17:12:51 onlfi_freeze: FTL - nbu_snap_freeze: Cannot turn on
snapshot; snapshot source=/oracle/ufs_r,
cache=/dev/rdisk/c4t1d11s4,snap error=11
```

- Look for stale snapshots by running the `/usr/opensv/netbackup/bin/driver/snaplist` command when there are no active backups running. If the `snaplist` command shows cache entries, there are stale snapshots. Nothing is displayed if there are no stale snapshots.

Example `snaplist` output:

```
id  ident      size      cached    minblk      err time
43  6515      8390970    0          0          0  11/16/00 13:31:36
device = /dev/rdisk/c1t6d0s0
cache  = /dev/rdisk/c1t6d0s7
```

- Use the `snapoff` command to remove the stale snapshot, as follows:

```
/usr/opensv/netbackup/bin/driver/snapoff id
```

Where *id* is the ID from the `snaplist` output (such as 43 in the preceding example).

- If a backup using the **VxFS\_Checkpoint** snapshot method failed, the NetBackup `bpbkar` process should automatically remove the clone. Sometimes, however, `bpbkar` is unable to remove the clone. In this case, you may see messages such as the following in the

`/usr/opensv/netbackup/logs/bpfiis log`:

```
15:21:45.716 [4236] <4> create_mount_point: INF - Created mount
point /tmp/_vtrax_test:4236
15:21:45.869 [4236] <2> onlfi_vfms_logf: INF - vxfs clone handle
: 9600344
15:21:45.870 [4236] <2> onlfi_vfms_logf: INF -
VxFS_Checkpoint_freeze: Cannot create checkpoint; status=17
15:21:45.872 [4236] <4> delete_mount_point: INF - Deleted mount
point /tmp/_vtrax_test:4236
15:21:45.873 [4236] <32> onlfi_freeze: FTL - VfMS error 11; see
following messages:
15:21:45.873 [4236] <32> onlfi_freeze: FTL - Fatal method error
was reported
15:21:45.873 [4236] <32> onlfi_freeze: FTL - vfm_freeze: method:
VxFS_Checkpoint, type: FIM, function: VxFS_Checkpoint_freeze
```

```
15:21:45.873 [4236] <32> onlfi_freeze: FTL - VxFS method error
17; see following message:
15:21:45.874 [4236] <32> onlfi_freeze: FTL -
VxFS_Checkpoint_freeze: Cannot create checkpoint; status=17
```

Remove the clone as follows.

---

**Note:** If the checkpoint is not removed, you cannot use **VxFS\_Checkpoint** to back up any data in the file system where the checkpoint is mounted.

---

- List the name of the checkpoint by entering the following VxFS command:

```
/usr/lib/fs/vxfs/fsckptadm list /file_system
```

Where *file\_system* is the name of the file system where the checkpoint is mounted. A sample output follows. In this example, */vtrax\_test* is the file system and *fi\_ckpt* is the name of the checkpoint.

```
/vtrax_test
fi_ckpt:
ctime = Mon Nov 12 10:08:13 2001
mtime = Mon Nov 12 10:08:13 2001
flags = largefiles
```

- Remove the checkpoint by entering the following:

```
/usr/lib/fs/vxfs/fsckptadm remove checkpoint /file_system
```

- If the checkpoint cannot be removed, unmount the checkpoint and retry the first step in this procedure.
- If a snapshot backup fails using TimeFinder, ShadowImage, or BusinessCopy method, there may be a VxVM clone left over from a previous backup. You may see messages similar to the following in the

```
/usr/opensv/netbackup/logs/bpfis log:
```

```
19:13:07.686 [14981] <2> onlfi_vfms_logf: INF - do_cmd: Command
failed with status=20: /usr/opensv/netbackup/bin/bpdgclone -g
wil_test -n vol01 -f /var/tmp/HDSTFCAAs7aOqD </dev/null
>/var/tmp/VfMSAAQ7aOqD 2>/var/tmp/VfMSBAAr7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file
/var/tmp/VfMSAAQ7aOqD (stdout):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- End of file
/var/tmp/VfMSAAQ7aOqD
```



```
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file
/var/tmp/VfMSBAAr7aOqD (stderr):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF -      clone group
and volume already exists
19:13:07.688 [14981] <2> onlfi_vfms_logf: INF - --- End of file
/var/tmp/VfMSBAAr7aOqD
```

NetBackup automatically creates VxVM clones for TimeFinder, ShadowImage, or BusinessCopy backups of the data that is configured over volumes. After the backup has completed, NetBackup removes the VxVM clone. In this case, a system crash or restart may have prevented the removal. Remove the clone as follows.

(Do the following on the client or alternate client, depending on the type of backup.)

- When no backups are running, use the following VxVM command to list any clones: `vxdg list`

The clone name is of the form `clone_disk_group_clone`.

- To remove the clone, enter the following:

```
/usr/opensv/netbackup/bin/bpdgclone -g disk_group -n volume -c
```

For example:

```
/usr/opensv/netbackup/bin/bpdgclone -g wil_test -n vol01 -c
```

Where `wil_test` is the name of the disk group and `vol01` is the name of the VxVM volume.

For more information on how to remove a VxVM clone, see the [NetBackup Snapshot Client Administrator's Guide](#). For `vxdg`, see the [Veritas Volume Manager Administrator's Guide](#).

- Before running the backup again, resynchronize the primary disk with the secondary disk. For assistance, see the [NetBackup Snapshot Client Administrator's Guide](#).
- If a snapshot backup fails using the FlashSnap or VVR snapshot method, a VxVM snapshot may be left over from a previous backup. You may see messages similar to the following in the `/usr/opensv/netbackup/logs/bpfis` log:

```
14:41:15.345 [22493] <32> onlfi_freeze: FTL - VfMS error 11; see
following messages:
14:41:15.345 [22493] <32> onlfi_freeze: FTL - Fatal method error
was reported
14:41:15.345 [22493] <32> onlfi_freeze: FTL - vfm_freeze_commit:
```

```
method: FlashSnap, type: FIM, function: FlashSnap_freeze_commit
14:41:15.345 [22493] <32> onlfi_freeze: FTL - VfMS method error
8; see following message:
14:41:15.345 [22493] <32> onlfi_freeze: FTL -
vxvm__find_ready_snapshot: Cannot find available snapshot mirror
```

NetBackup automatically creates VxVM snapshots for backups of the data that is configured over volumes. After the backup completes, NetBackup removes the VxVM snapshot. In this case, a system crash or restart may have prevented the removal. Remove the snapshot as follows.

For FlashSnap:

(Do the following on the client or alternate client, depending on the type of backup.)

- Find the VxVM disk group:

```
vxvg list
```

The format of the disk group name is as follows:

```
primaryhost_diskgroup_split
```

If `vxvg list` does not show the disk group, the group might have been deported. You can discover all the disk groups including deported ones by entering:

```
vxdisk -o alldgs list
```

The disk groups that are listed in parentheses are not imported on the local system.

- Deport the VxVM disk group:

```
vxvg deport primaryhost_diskgroup_split
```

Enter the following on the primary (original) client:

- Import and join the VxVM disk group:

```
vxvg import primaryhost_diskgroup_split
vxrecover -g primaryhost_diskgroup_split -m
vxvg join primaryhost_diskgroup_split diskgroup
```

- Start the volume and snap back the snapshot volume:

```
vxvol -g primaryhost_diskgroup_split start
SNAP_diskgroup_volume
vxassist snapback SNAP_diskgroup_volume
```

For VVR, on the alternate client:

- Enter the following to display unsynchronized mirror disks:

```
vxprint -g diskgroup
```

- Enter the following to resynchronize the mirror disks:

```
vxassist -g diskgroup -v volume snapback
```

- When you use a snapshot method such as VxFS\_Checkpoint to back up a Veritas File System (VxFS), the backup fails if the VxFS license has expired. Messages such as the following appear in the `/usr/openv/netbackup/logs/bpffi` log:

```
11:37:42.279 [24194] <2> onlfi_vfms_logf: INF -
VxFS_Checkpoint_freeze: Cannot open checkpoint; status=100
11:37:42.283 [24194] <4> delete_mount_point: INF - Deleted mount
point /tmp/_vrts_frzn_img_test1_24194
11:37:42.283 [24194] <32> onlfi_freeze_fim_fs: FTL - VfMS error
11; see following messages:
11:37:42.283 [24194] <32> onlfi_freeze_fim_fs: FTL - Fatal
method error was reported
11:37:42.284 [24194] <32> onlfi_freeze_fim_fs: FTL - vfm_freeze:
method: VxFS_Checkpoint, type: FIM, function:
VxFS_Checkpoint_freeze
11:37:42.284 [24194] <32> onlfi_freeze_fim_fs: FTL - VfMS method
error 100; see following message:
11:37:42.284 [24194] <32> onlfi_freeze_fim_fs: FTL -
VxFS_Checkpoint_freeze: Cannot open checkpoint; status=100
```

Obtain a new VxFS license and retry the backup.

- If the backup is enabled for instant recovery with either the VxVM or VVR snapshot method, your VxVM mirrors may not be properly configured. In this case, you may see the following in the `/usr/openv/netbackup/logs/bppfi` log on the client (when verbose mode is set high).

```
13:43:39.095 [16375] <2> onlfi_vfms_logf: INF - Executing
command:
13:43:39.095 [16375] <2> onlfi_vfms_logf: INF -
/usr/sbin/vxprint -g rootdg -q -t -e 'assoc="pfi_concat"'
</dev/null >/var/tmp/VfMSAA Arja4.F 2>/var/tmp/VfMSBAAsja4.F
13:43:39.215 [16375] <2> onlfi_vfms_logf: INF -
pfi_find_snapdone: 0 SNAPDONE plexes found
```

```
13:43:39.215 [16375] <2> onlfi_vfms_logf: INF - Executing
command:
13:43:39.215 [16375] <2> onlfi_vfms_logf: INF -
/usr/sbin/vxassist -g rootdg snapprint pfi_concat </dev/null
>/var/tmp/VfMSAAArja4.F 2>/var/tmp/VfMSBAAsja4.F
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF - 0 active plexes
for /rootdg/pfi_concat: 0 are PFI 0 non-PFI
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF -
pfi_find_active.3309: exiting with VXVM_E_SYS = 3
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF -
pfi_snapshot.3866: No PFI snapshot. err= 3
```

Configure the VxVM mirrors as described in the Instant Recovery chapter of the [NetBackup Snapshot Client Administrator's Guide](#).

- When you use the VxFS\_Checkpoint snapshot method, the backup fails if the client's file system does not support mountable checkpoints using the Storage Checkpoint feature. Messages such as the following appear in the `/usr/opensv/netbackup/logs/bpfis` log:

```
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - VfMS error
11; see following messages:
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - Fatal
method error was reported
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - vfm_freeze:
method: VxFS_Checkpoint, type: FIM, function:
VxFS_Checkpoint_freeze 14:54:27.531 [23563] <32>
onlfi_freeze_fim_fs: FTL - VfMS method error 2; see following
message:
14:54:27.531 [23563] <32> onlfi_freeze_fim_fs: FTL - open_ckpt:
Cannot open checkpoint on /mnt_vxvm/2G_concat :
fsckpt_get_api_version returns 1; mountable checkpoints not
supported with this version
```

Do one of the following:

- Upgrade the client file system to a version that supports mountable VxFS Storage Checkpoints.
- Configure the policy with a snapshot method that supports the client's current file system.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 157

**Message:** suspend requested by administrator

**Explanation:** Status code 157 is an informational message, which indicates that the administrator suspended the job from the Activity Monitor. The job is in the suspended state in the Activity Monitor. It can be resumed from the last checkpoint by the administrator.

**Recommended Action:** The administrator can resume the job from the last checkpoint from the Activity Monitor.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 158

**Message:** failed accessing daemon lock file

**Explanation:** The process cannot lock its lock file because an error was received from a system call. This lock file synchronizes process activities (for example, it prevents more than one daemon from running at a time).

**Recommended Action:** Do the following, as appropriate:

- Examine the NetBackup error log to determine why the system call failed. Then correct the problem. It may be a permission problem.
- If the error log does not show the error, create a debug log directory for `bprd` or `bpdsm` (depending on which process encountered the error). Increase the unified logging level if `nbpem`, `nbjm`, or `nbrb` encountered the error. Use the `vxlogcfg` command as explained in the following topic:  
See "About unified logging" in the [NetBackup Logging Reference Guide](#).  
Retry the operation and check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 159

**Message:** licensed use has been exceeded

**Explanation:** A configuration limit was exceeded.

For example, a job fails with this error code if a policy is set up that specifies the following:

- A storage unit that is on a SAN media server
- A client that is not the SAN media server itself

SAN media servers can only back up themselves.

This status code is used when the creation of a storage unit on a SAN media server fails because **On demand only** is not selected. **On demand only** is required for storage units on a SAN media server.

**Recommended Action:** To determine the cause of the error, examine the NetBackup All Log Entries report for the command that was run. See also the Activity Monitor details for informative messages.

If the job fails on a SAN media server storage unit, ensure that only the local client is specified in the policy. If remote clients are specified in the policy, do one of the following: remove them and place them in a policy that specifies a different storage unit or change the storage unit for that policy.

If you want to back up remote clients by using the SAN media server, you can purchase a regular NetBackup media server license.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 160

**Message:** authentication failed

**Explanation:** One of the following occurs:

- Two systems try to authenticate one another.
- An initialization of the authentication libraries fails.
- Communication to the authentication daemon (`nbatd`) fails.
- Authentication of saved credentials fails.

**Recommended Action:** Do the following as appropriate in the order listed:

- Add back the names that were removed and retry the operation.
- Create the following debug log directories for the processes that are involved in authentication between NetBackup systems:
  - **Server:** `bprd`, `bpdbm`, and `bpcd`.
  - **Client:** `bpbackup`, `bprestore`, and `bpbkar`.

Retry the operation and check the logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 161

**Message:** Evaluation software has expired.

**Explanation:** The time that was allowed for the NetBackup evaluation software ended.

See [www.veritas.com](http://www.veritas.com) for ordering information.

**Recommended Action:** Obtain a licensed copy of NetBackup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 162

**Message:** incorrect server platform for license

**Explanation:** The platform identifier in the license key does not match the platform type on which the key was installed.

**Recommended Action:** Ensure that you use a license key that is intended for the platform on which you plan to install.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 163

**Message:** media block size changed prior resume

**Explanation:** Status code 163 is an informational message. It indicates that the media block size was changed before a backup job from the last checkpoint resumed. Since the media block size must be consistent, the job was restarted from the beginning.

**Recommended Action:** Check the Activity Monitor job details for the job ID of the restarted job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 164

**Message:** unable to mount media because it is in a DOWN, or otherwise not available

**Explanation:** A restore was tried and the volume required for the restore was in a DOWN drive in a robot. Or, the slot is empty that should contain the volume.

**Recommended Action:** Do the following, as appropriate:

- If volume is in a DOWN drive, remove it and place it in its designated slot. Then, retry the restore.
- If the volume is in the wrong slot, use a robot inventory option to reconcile the contents of the robot with the volume configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 165

**Message:** NB image database contains no image fragments for requested backup id/copy number

**Explanation:** A restore was tried and NetBackup has no record of the fragments that are associated with the backup ID that has the files.

**Recommended Action:** Check the NetBackup Problems report for additional information about the error. For detailed troubleshooting information, create a debug log directory for either `bpdm` or `bptm` (whichever applies) and retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 166

**Message:** backups are not allowed to span media

**Explanation:** An end of media (EOM) was encountered while the backup image was written. The backup was terminated because the NetBackup `DISALLOW_BACKUPS_SPANNING_MEDIA` option was present in `bp.conf` (on UNIX) or in the registry (on Windows). The backup is retried automatically with a different volume if the backup tries attribute allows it in the NetBackup global attribute configuration.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 167

**Message:** cannot find requested volume pool in EMM database

**Explanation:** A backup to a nonrobotic drive was tried and the tape manager (`bptm`) cannot find or add the specified volume pool.



**Recommended Action:** Verify the Media and Device Management volume configuration. Check the NetBackup Problems report for more information about the error. For detailed troubleshooting information, create a `bptm` debug log directory and retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 168

**Message:** cannot overwrite media, data on it is protected

**Explanation:** A backup was tried to a volume that cannot be overwritten because it contains the data that by default NetBackup does not overwrite. (This data includes items such as tar, cpio, and ANSI.)

**Recommended Action:** Replace the volume with a new one or set the NetBackup `ALLOW_MEDIA_OVERWRITE` option to the appropriate value.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 169

**Message:** Media ID is either expired or will exceed maximum mounts

**Explanation:** A backup or a catalog backup was tried and the volume selected for use has reached its maximum number of mounts. The maximum number is specified in the Media and Device Management volume configuration. For a regular backup, the volume is automatically set to the SUSPENDED state and not used for further backups. For a NetBackup catalog backup, the operation terminates abnormally.

**Recommended Action:** If the volume was suspended, wait until it expires and then replace it. For NetBackup catalog backups, replace the media.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 170

**Message:** third party copy backup failure

**Explanation:** Usually indicates a problem with the `3pc.conf` file or the `mover.conf` file. (For detailed causes, see recommended actions.)

For more information on these files, see the *NetBackup Snapshot Client Configuration* document available at the following location:

[https://www.veritas.com/content/support/en\\_US/article.TECH51377.html](https://www.veritas.com/content/support/en_US/article.TECH51377.html)

For help accessing this document, see Snapshot Client Assistance in the [NetBackup Snapshot Client Administrator's Guide](#).

**Recommended Action:** Do the following, as appropriate:

- If a non third-party copy device is listed in `3pc.conf` file, correct it or remove the non third-party copy device entry.
- If an incorrect LUN is specified in the `3pc.conf` file or the device does not exist, correct the `3pc.conf` file as appropriate.
- If an appropriate `mover.conf` file (with or without file name extension) cannot be found, the `/usr/opensv/netbackup/logs/bptm` log may show the following:

```
09:51:04 [22281] <2> setup_mover_tpc: no
mover.conf.vertex_std_tpc or mover.conf file exists, cannot
perform TPC backup
09:51:04 [22281] <16> bptm: unable to find or communicate with
Third-Party-Copy mover for policy vertex_std_tpc
```

Make sure that an appropriate `mover.conf` file exists in `/usr/opensv/netbackup` on the media server. This file can be any of the following:

- `mover.conf.policy_name` file, where *policy\_name* exactly matches the name of the policy.
- `mover.conf.storage_unit_name`, where *storage\_unit\_name* exactly matches the name of the storage in the **Backup Policy Management Policy attributes** dialog box (such as `nut-4mm-robot-tl4-0`).
- `mover.conf` file (no extension) for the configurations that have only one third-party copy device.

Note that NetBackup looks for an appropriate `mover.conf` file in the order.

- If the SCSI pass-through path of the third-party copy device, as entered in the `mover.conf` file, does not exist, the `bptm` log may show the following:

```
09:50:12 [22159] <16> setup_mover_tpc: open of passthru path
/dev/sg/cXtXlX failed, No such file or directory
09:50:12 [22159] <16> bptm: unable to find or communicate with
Third-Party-Copy mover for policy vertex_std_tpc
```

Correct the SCSI pass-through path of the third-party copy device that is entered in the `mover.conf` file.

- If the third-party copy device returned an error, you may see either of the following messages in `/usr/opensv/netbackup/logs/bptm` log:

cannot process extended copy error due to truncated sense data,  
 may be HBA problem  
 disk error occurred on extended copy command, key = 0x0, asc =  
 0x0, ascq = 0x0

(where key, asc, and ascq are all zero)

Your host-bus adapter (HBA) and its driver may need to be updated, or  
 NetBackup Snapshot Client may not support them. The supported host-bus  
 adapters are listed.

See the [NetBackup Release Notes](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge  
 Base about this status code.

## NetBackup status code: 171

**Message:** media ID must be 6 or less characters

**Explanation:** An operation that suspends or freezes a media ID (for example,  
 bpmedia). was tried. The media ID is longer than six alphanumeric characters.

**Recommended Action:** Retry the command with a valid media ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge  
 Base about this status code.

## NetBackup status code: 172

**Message:** cannot read media header, may not be NetBackup media or is corrupted

**Explanation:** When you loaded a volume for a backup or restore, the tape manager  
 (bptm), did not find the expected tape header. This error can mean that a robotic  
 device volume is not in the slot number that is in the Media and Device Management  
 volume configuration. It also can mean that a read error (I/O error) occurred.

**Recommended Action:** Do the following, as appropriate:

- If the volume is in a robot that supports bar codes, verify the robot contents by  
 using a robot inventory option.
- If the volume was mounted on a nonrobotic drive, verify that the correct volume  
 was mounted and assigned.
- Check the NetBackup Problems report. If it shows a fatal read error, try the  
 operation again with another drive, if possible.
- If your configuration has multiple servers or HBAs with access to your tape  
 services, make sure that the SCSI Reserve or Release is configured correctly.  
 (Most likely, the tape services configuration is an SSO configuration.)

For more information on the storage server, please see the *NetBackup Administrator's Guide, Volume II*, available from the following location:

<http://www.veritas.com/docs/DOC5332>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 173

**Message:** cannot read backup header, media may be corrupted

**Explanation:** When the tape manager (`bptm`) searches for a backup image to restore, the following occurs: it cannot find the correct backup ID at the position on the media where NetBackup expected it. This status code can indicate a drive hardware problem.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues as to what caused the error.
- Try the restore on another drive if possible.
- For detailed troubleshooting information, create a debug log directory for `bptm` and retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 174

**Message:** media manager - system error occurred

**Explanation:** An abnormal condition caused a tape manager (`bptm`) or disk manager (`bpdm`) failure.

On UNIX, the file list that NetBackup generates for snapshot copy may not have enough information to restore from the NetBackup `tar` copy. For example, block number information is not correct because the NetBackup `tar` copy is not yet created.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report to see if it shows the cause of the problem. If you see a Problems report message similar to the following, save all logs and contact Veritas Technical Support:

```
attempted to write 32767 bytes, not a multiple of 512
```

- On UNIX, if this error occurs during a restore, the tape drive may be incorrectly configured. It may be configured to write in fixed-length mode when it should write in variable length mode.

Verify your drive's configuration by comparing it to what is recommended in the [NetBackup Device Configuration Guide](#).

If your configuration incorrectly specifies fixed-length mode, change it to variable length mode and suspend the media that were written on that device. The images that were written to those media may be restorable (platform dependent), but single file restores are likely to fail.

- If the problem occurs with a particular client only, verify that the client binaries are correct, especially for `bpcd`.
- If you can read or write any other images on this media, check the following reports for clues:
  - Images on Media report
  - Media Contents report
- Verify the following:
  - The media, by using the NetBackup image verify option.
  - That you used the correct media type for the device.
- Check the system or the console log for errors (on UNIX) or the Event Viewer Application log (on Windows).
- For detailed debug information, create a debug log directory for either `bptm` or `bpdm` (whichever applies) and retry the operation. Check the resulting debug log.

On UNIX, if the `bptm` debug log shows an error similar to the following, the tape drive is configured to write in fixed-length mode rather than variable length mode.

```
00:58:54 [2304] <16> write_data: write of 32768 bytes indicated
only 29696 bytes were written, errno = 0
```

The image being written encountered the end-of-media.

- If the backup was configured for an OpenStorage disk storage unit, the OpenStorage vendor's plug-in may not be installed on all media servers in the storage unit's media server list. Either install the vendor plug-in on all of the media servers or remove from the list the servers that do not have the plug-in installed.
- On UNIX, if this error occurs during a restore, refresh the **Backup, Archive, and Restore** client console and retry the restore. This action refreshes the file

list displayed in the client console and passes the correct information about the selected files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 175

**Message:** not all requested files were restored

**Explanation:** When the `bptm` or the `bpdm` process restores files from an image, it detected a fatal error condition and terminated the restore before it completed. Under normal circumstances, this error should not occur.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report and the status lot or the progress log on the client for additional information about the error.
- For detailed troubleshooting information, create a debug log directory for either `bptm` or `bpdm` (whichever applies) and retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 176

**Message:** cannot perform specified media import operation

**Explanation:** The tape manager (`bptm`) detected an error condition when it tried to import a specific backup image.

Possible reasons for this error are as follows:

- Media ID is already active in the NetBackup media catalog on this server
- Media ID is not in the volume configuration
- Fatal tape manager (`bptm`) error occurred
- Total image was not obtained from Phase 1 of import
- The barcode and media ID do not match in the volume database. One possible reason for a mismatch is when using tapes previously written by a different barcode, labels are placed into an ACSLS library using a new barcode label. Another possible reason is when the administrator attempts to change the media ID field (using `vmchange`) to match the RVSN. When the inventory is updated, the barcode and media ID are synchronized.

**Recommended Action:** Check the NetBackup Problems report to find the exact cause of the failure and try the following:

- If the media ID is already active, duplicate all images on the original media ID to another volume. Then, manually expire the original media and redo the import.
- If the media ID is not present in the volume configuration, add it.
- If you received a fatal `bptm` error, verify that the following are active: the NetBackup Volume Manager (`vmd`) on UNIX or the NetBackup Volume Manager on Windows.
- If the entire image is not present, perform import phase 1 on the media IDs that have the remainder of the image.
- If the barcode and media ID are a mismatch, use a barcode label that matches the recorded media ID. Tapes can then be mounted in a drive with AVRDC running so that the recorded media ID is displayed. Then, a barcode with that label needs to be placed on the tape.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 177

**Message:** could not deassign media due to Media Manager error

**Explanation:** The tape manager (`bptm`) cannot successfully unassign a media ID.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for the cause of the problem.
- Verify that the NetBackup Volume Manager (`vmd`) is active on UNIX or the NetBackup Volume Manager service is active on Windows.
- For detailed troubleshooting information, create a debug log directory for `bptm` and retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 178

**Message:** Media ID is not in NetBackup volume pool

**Explanation:** NetBackup tried a backup of its catalogs and the media ID that was specified for the catalog backup was not in the NetBackup volume pool. Volumes for catalog backups must be in the NetBackup volume pool.

**Recommended Action:** Check the Media and Device Management volume configuration to verify that the media IDs are present and in the NetBackup volume pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 179

**Message:** density is incorrect for the media ID

**Explanation:** An operation such as "list contents" was tried on an invalid media ID, such as a cleaning tape. Another possibility: a media ID in the NetBackup catalog backup configuration does not match the media type that was entered in the volume configuration.

**Recommended Action:** Check the volume configuration and the NetBackup catalog backup configuration and correct any problems found.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 180

**Message:** tar was successful

**Explanation:** `tar` returned a successful exit status.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 181

**Message:** tar received an invalid argument

**Explanation:** One of the parameters that was passed to `tar` was not valid.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX client:
  - Ensure that the `nbtar` command in `/usr/openv/netbackup/bin` is the one provided by NetBackup. If you are in doubt, reinstall it.
  - Check `/usr/openv/netbackup/bin/version` on the client to verify that the client is running the correct level software. If the software is not at the correct level, update the software per the directions in the NetBackup release notes.



- On a Windows client, create a `tar` debug log directory, retry the operation, and check the log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 182

**Message:** tar received an invalid file name

**Explanation:** `tar` cannot write to the file that is specified with the `-f` parameter.

**Recommended Action:** Do the following, as appropriate:

- Create a `bpcd` debug log directory on the client .
- On a Windows client, create a `tar` debug log directory.
- Increase the logging level on the client:
  - On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
- Rerun the operation, check the resulting debug logs for the parameters that were passed to `tar` and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 183

**Message:** tar received an invalid archive

**Explanation:** The data that was passed to `tar` was corrupt.

**Recommended Action:** Do the following, as appropriate:

- If the problem is with a UNIX client, create a `/usr/openv/netbackup/logs/tar` debug log directory on the client and rerun the operation.
  - Check the `tar` debug log file for any error messages that explain the problem.
  - Restart the client to see if it clears the problem.
  - When you finish with your investigation of the problem, delete the `/usr/openv/netbackup/logs/ tar` directory on the client.

- If the problem is with a Microsoft Windows client, do the following in the order presented:
  - Create a `bpcd` debug log directory on the client.
  - On a Windows client, create a `tar` debug log directory.
  - Increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
  - Rerun the operation and check the resulting debug logs.
  - Restart the client to see if it clears the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 184

**Message:** tar had an unexpected error

**Explanation:** A system error that occurred in `tar`.

**Recommended Action:** Do the following, as appropriate:

- If the problem is with a UNIX client, create a `/usr/openv/netbackup/logs/tar` debug log directory on the client and rerun the operation.
  - Check the `tar` debug log file for any error messages that explain the problem.
  - Restart the client to see if it clears the problem.
  - When you finish your investigation of the problem, delete the `/usr/openv/netbackup/logs/tar` directory on the client.
- If the problem is with a Microsoft Windows client:
  - Create a `bpcd` debug log directory on the client .
  - Increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
  - On a Windows client, create a `tar` debug log directory.
  - Retry the operation and check the resulting debug logs.
  - Restart the client to see if it clears the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 185

**Message:** tar did not find all the files to be restored

**Explanation:** The `tar` file list contained files that were not in the image.

**Recommended Action:** Do the following, as appropriate:

- If the problem is with a UNIX client:
  - Enable `bpcd` debug logging by creating the `/usr/openv/netbackup/logs/bpcd` directory on the client.
  - Rerun the operation, check the resulting `bpcd` log file for the parameters that were passed to `nbtar`, and contact Technical Support.
- If the problem is with a Microsoft Windows client:
  - Create a `bpcd` debug log directory on the client.
  - Increase the debug or log level.  
See "Changing the logging level on Windows clients" in the [NetBackup Logging Reference Guide](#).
  - On a Windows client, create a `tar` debug log directory.
  - Retry the operation.
  - Check the resulting debug logs for the parameters that were passed to `tar` and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 186

**Message:** tar received no data

**Explanation:** NetBackup did not send data to `tar`.

**Recommended Action:** Do the following, as appropriate:

- Retry the operation and check the status or the progress log on the client for any error messages that reveal the problem.
- Verify that the tape is available and readable.
- Verify that the drive is in an UP state. Use the Device Monitor.
- For detailed troubleshooting information:
  - Create a `bptm` debug log on the server.
  - On a Windows client, create a `tar` debug log.

- Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 189

**Message:** the server is not allowed to write to the client's file systems

**Explanation:** The client does not allow writes from the server.

**Recommended Action:** Perform the following to perform restores or install software from the server:

- On a UNIX client, delete `DISALLOW_SERVER_FILE_WRITES` from the `/usr/opensv/netbackup/bp.conf` file.
- On a Microsoft Windows client, select **Allow server-directed restores** on the **General** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and select **NetBackup Client Properties** from the **File** menu.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 190

**Message:** found no images or media matching the selection criteria

**Explanation:** A verify, duplicate, or import was tried and no images that matched the search criteria were found in the NetBackup catalog.

**Recommended Action:** Change the search criteria and retry.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 191

**Message:** no images were successfully processed

**Explanation:** One of the following has occurred:

- A verify, duplicate, Auto Image Replication, automatic import, or import was tried and failed for all selected images.
- If the `STS_EFILESYSTEM` error code appears (error 2060063) for BasicDisk or AdvancedDisk, the file system is not configured correctly. The Allocation Unit Size of the NTFS file system is too small for the BasicDisk or AdvancedDisk

data writes. Or, the maximum fragment size that NetBackup configures is too large.

- If a backup or duplicate job is configured with a retention level greater than 25 and the storage unit specified in the policy is managed by a media server that runs a version of NetBackup previous to NetBackup 8.0, the backup jobs associated with the policy fail.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for the cause of the error. To obtain detailed troubleshooting information, create an `admin` debug log directory and retry the operation. Check the resulting debug log.
- If the backup or duplicate job failed for a policy configured with a retention level greater than 25, you can either upgrade the media server to NetBackup 8.0 or later or set the retention level between 0 and 25. Note that the retention period for level 25 is always set to expire immediately and this value cannot be changed.
- If the error was encountered during duplication of backups, check the duplication progress log to help determine the root cause of the problem.
- An Auto Image Replication job may cause this error. If the storage lifecycle policy names or data classifications do not match the originating domain and the target domain, the import job fails. Failed imports appear in the Problems report when it is run on the target master server. The image is expired and deleted during catalog cleanup. Note that the originating domain does not track failed imports.

More information is available about troubleshooting this problem:

For more information on troubleshooting this problem, please see the About Troubleshooting Auto Image Replication topic of the [NetBackup Troubleshooting Guide](#).

- An automatic import job may cause this error. This job is an import job that shows a storage lifecycle policy name.

More information is available about troubleshooting this problem:

For more information on troubleshooting this problem, please see the About Troubleshooting Auto Image Replication topic of the [NetBackup Troubleshooting Guide](#).

- If a Vault job encountered the error responsible for the duplication, check the `duplicate.log` files in your `sidxxx` directories to determine the root cause:

UNIX:

`/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows:

`install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where xxx is the session ID)

- Reduce the maximum fragment size on the storage unit that writes to this file system. This value is typically less than 20 GB. But you may need to adjust the maximum fragment size as necessary until the STS\_EFILESYSTEM errors no longer occur. The value is based on how much data that the storage unit writes to the image.

To change this value, in the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Storage**. Then in the right pane, double-click the storage unit for this file system. In the **Change Storage Unit** dialog box, change the value of the Maximum Fragment Size to 20480 MB (20 GB) by checking the **Reduce fragment size to** checkbox and entering the new value.

- Increase the Allocation Unit Size by reconfiguring the file system. This usually requires that you format the file system, so this action may not be a feasible for an existing file system. Consider this when you create a new file system for BasicDisk images or AdvancedDisk images. Because setting this value is different on each OS file system, refer to the appropriate OS or file system documentation for instructions.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 192

**Message:** VxSS authentication is required but not available

**Explanation:** On one side of a NetBackup network connection, the system requires VxSS authentication. On the other side of the connection, the other system is not configured to use VxSS. VxSS authentication is used with the NetBackup Access Control feature (NBAC). The connection was terminated because VxSS authentication cannot be completed.

**Recommended Action:** Make sure that both systems are configured to use NetBackup Access Control VxSS authentication with each other. Or, make sure that both systems are not configured to use VxSS with each other. The first thing to check is the Use VxSS Host properties value on each system. If one is configured for REQUIRED, the other must be configured for REQUIRED or AUTOMATIC. If one is configured for PROHIBITED, the other must be configured for PROHIBITED or AUTOMATIC.

See the [NetBackup Administrator's Guide, Volume I](#), for the following information: how to set the Access Control-related host properties, and how to configure a system to use Access Control.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 193

**Message:** VxSS authentication is requested but not allowed

**Explanation:** On one side of a NetBackup network connection, the system requires VxSS authentication. The system on the other side of the connection is not configured to use VxSS. VxSS authentication is used with the NetBackup Access Control feature (NBAC). The connection has been terminated because VxSS authentication cannot be completed.

**Recommended Action:** Make sure that both systems are configured to use NetBackup Access Control VxSS authentication with each other. Or, make sure that both systems are not configured to use VxSS with each other. The first thing to check is the Use VxSS Host properties value on each system. If one is configured for REQUIRED, the other must be configured for REQUIRED or AUTOMATIC. If one is configured for PROHIBITED, the other must be configured for PROHIBITED or AUTOMATIC.

See the [NetBackup Administrator's Guide, Volume I](#), for the following information: how to set the Access Control-related host properties how to configure a system to use Access Control.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 194

**Message:** the maximum number of jobs per client is set to 0

**Explanation:** The NetBackup **Maximum jobs per client** global attribute is currently set to 0. Set the value to 0 to disable backups and archives.

**Recommended Action:** To enable backups and archives, change the **Maximum jobs per client** value to the wanted nonzero setting. This attribute is on the **Global NetBackup Attributes** tab in the **Master Server Properties** dialog box.

See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 195

**Message:** client backup was not attempted

**Explanation:** A backup job was in the NetBackup scheduler but was not tried.

**Recommended Action:** Do the following, as appropriate:

- Retry the backup either immediately with a manual backup or allow the normal scheduler retries.
- For additional information, check the All Log Entries report. For detailed troubleshooting information, increase the logging level for the diagnostic and debug logs for `nbpem`, `nbjm`, and `nbrb`.

Use the `vxlogcfg` command as explained in the following topic:

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

After the next backup try, check the logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 196

**Message:** client backup was not attempted because backup window closed

**Explanation:** A backup or an archive operation that the backup scheduler queued was not tried because the backup window was no longer open.

**Recommended Action:** Do the following, as appropriate:

- If possible, change the schedule to extend the backup window for this combination of policy and schedule so it does not occur again.
- If the backup must be run, use the **Manual Backup** command on the **Policy** menu in the **Backup Policy Management** window to perform the backup. Manual backups ignore the backup window.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 197

**Message:** the specified schedule does not exist in the specified policy

**Explanation:** A user backup or archive request specified the exact policy and schedule to use when a backup is performed. The policy exists but does not contain the schedule.

- On Microsoft Windows clients, you can specify a policy or schedule on the **Backups** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and select **NetBackup Client Properties** on the **File** menu.



- On UNIX clients, you can specify a policy or schedule by using the `bp.conf` options, `BPBACKUP_POLICY` or `BPBACKUP_SCHEDULE`.

**Recommended Action:** Do the following, as appropriate:

- Check the client progress log (if available) to determine the policy and schedule that were specified.
- Check the configuration on the master server to determine if the schedule is valid for the policy. If the schedule is not valid, either add the schedule to the policy configuration or specify a valid schedule on the client.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 198

**Message:** no active policies contain schedules of the requested type for this client

**Explanation:** A user backup or archive was requested, and this client is not in a policy that has a user backup or archive schedule.

**Recommended Action:** Determine if the client is in any policy that has a schedule of the appropriate type (either user backup or archive).

- If the client is in such a policy, check the general policy attributes to verify that the policy is set to active.
- If the client is not in such a policy, do either of the following:
  - Add a schedule of the appropriate type to an existing policy that has this client.
  - Create a new policy that has this client and a schedule of the appropriate type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 199

**Message:** operation not allowed during this time period

**Explanation:** A user backup or archive was requested and this client is not in a policy that has the following: a user backup or archive schedule with an open backup window. This error implies that an appropriate policy and schedule combination exists for this client.

**Recommended Action:** Determine the policies to which this client belongs that also have a schedule of the appropriate type (either user backup or archive).

- If possible, retry the operation when the backup window is open.
- If the backup window is not open during appropriate time periods, adjust a backup window for a schedule in one of the policies.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 200

**Message:** scheduler found no backups due to run

**Explanation:** When the NetBackup scheduler process (`nbpem`) checked the policy and the schedule configuration, it did not find any clients to back up.

This error may be due to the following:

- No backup time windows are open (applies only to full and to incremental schedules).
- Policies are set to inactive.
- The clients were recently backed up and are not due for another backup (based on Frequency setting for the schedules).
- Policies do not have any clients.

**Recommended Action:** Usually, this message can be considered informational and does not indicate a problem. However, if you suspect a problem, do the following:

- Examine the NetBackup All Log Entries report for any messages in addition to the one that indicates the scheduler found nothing to do.
- Examine the policy configuration for all policies or the specific policy in question to determine if any of the reasons in the Explanation section apply.
- To obtain detailed troubleshooting information, increase the unified logging level for the diagnostic and debug logs.

Use the `vxlogcfg` command as explained in the following procedure:

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

Retry the operation and check the resulting logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 201

**Message:** handshaking failed with server backup restore manager

**Explanation:** A process on the master server encountered an error when it communicated with the media host (can be either the master or a media server). This error means that the master and the media server processes were able to initiate communication, but were not able to complete them. This problem can occur during a backup, restore, or media list in a single or a multiple server configuration.

**Recommended Action:** Do the following, as appropriate:

- Determine the activity that encountered the handshake failure by examining the NetBackup All Log Entries report for the appropriate time period. If there are media servers, determine if:
  - The handshake failure was encountered between the master and a media server.  
or
  - Only the master server was involved.
- If necessary, create the following debug log directories and increase the logging level:
  - `bpcd` on the NetBackup media host (can be either the master or a media server).
  - If the error was encountered during a backup operation, increase the logging level for the diagnostic and debug logs for `nbpem`, `nbjm`, and `nbrb`.  
Use the `vxlogcfg` command as explained in the following procedure:  
See "About unified logging" in the [NetBackup Logging Reference Guide](#).
  - If the error was encountered during a restore operation, `bprd` on the master server.
  - If the error was encountered during a media list operation, `admin` in the NetBackup `logs/admin` directory on the master server.
- Status code 201 may occur if `nbjm` fails after it connects to `bpbrm` or `bpmount` but before the policy file list is sent. Examine the `nbjm` unified log (originator ID 117) or the `bpbrm` or the `bpmount` legacy logs for more detail on the cause of the error.
- Retry the operation and examine the resulting debug logs for information on why the error occurred.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 202

**Message:** timed out connecting to server backup restore manager

**Explanation:** A master server process that tried to initiate communications with the media host timed out (can be either the master or a media server). This problem can occur during a backup or restore in either a single or a multiple server configuration.

**Recommended Action:** Determine which activity encountered the connection timeout failure by examining the All Log Entries report for the appropriate time period. If there are media servers, determine if the timeout occurred between the master and a media server or if only the master was involved.

- Verify that the schedule specifies the correct storage unit.
- Run the `ping` command from one host to another by using the following combinations:
  - From the master server, ping the master and all media servers by using the host names that are found in the storage unit configuration.
  - From each of the media servers, ping the master server by using the host name that is specified in the NetBackup server list. On a UNIX or Linux server, the master is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box.  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
- Verify that the master server can communicate with `bpcd` on the host that has the storage unit.
- Perform the following procedures:
  - See "Testing the media server and clients" in the [NetBackup Troubleshooting Guide](#).
  - See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- If necessary, create debug log directories for the following processes and retry the operation. Then, check the resulting debug logs on the master server:
  - If the error occurred during a backup operation, increase the logging level for the diagnostic and debug logs for `nbpem`, `nbjm`, and `nbrb`.  
Use the `vxlogcfg` command as explained in the following procedure:  
See "About unified logging" in the [NetBackup Logging Reference Guide](#).  
Also, check the `bpcd` legacy debug logs.
  - If the error occurs during a restore operation, check the `bprd` debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 203

**Message:** server backup restore manager's network is unreachable

**Explanation:** A process on the master server cannot connect to a particular host on the network when it tries to initiate communication with the media host. This problem can occur during a backup or restore in either a single or a multiple server configuration.

**Recommended Action:** Determine which activity encountered this failure by examining the All Log Entries report for the appropriate time frame. If there is more than one NetBackup server (one or more media servers), determine the following: if the failure was between the master and a media server or if only the master server was involved. Run the `ping` command from one host to another by using the following combinations:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
- From each of the media servers, ping the master server host by using the host name that is specified in the NetBackup server list. On a UNIX or Linux server, the master is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog.  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
- Perform the following procedures:  
See "Testing the media server and clients" in the [NetBackup Troubleshooting Guide](#).  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- If necessary, create debug log directories for `bprd` and retry the operation. Then, check the resulting debug logs on the master server. If the error occurred during a restore, check the `bprd` debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 204

**Message:** connection refused by server backup restore manager

**Explanation:** The media host refused a connection on the port number for `bpcd`. This error can be encountered during a backup or restore.

**Recommended Action:** Run the `ping` command from one host to another by using the following combinations:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
- From each of the media servers, ping the master server by using the name that was specified in the NetBackup server list. On a UNIX or Linux server, this master is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box. The following topic shows how to access this dialog box:  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
- On UNIX and Linux servers, verify that the `bpcd` entries in `/etc/services` or NIS on all the servers are identical. Verify that the media host listens on the correct port for connections to `bpcd`. To verify, run one of the following commands (depending on platform and operating system):

```
netstat -a | grep bpcd
```

```
netstat -a | grep 13782 (or the value that was specified during the install)
```

```
rpcinfo -p | grep 13782 (or the value that was specified during the install)
```

On UNIX and Linux servers, it may be necessary to change the service number for the following: `bpcd` in `/etc/services` and the NIS services map and send `SIGHUP` signals to the `inetd` processes on the clients.

```
/bin/ps -ef | grep inetd
```

```
kill -HUP the_inetd_pid
```

or

```
/bin/ps -aux | grep inetd
```

```
kill -HUP the_inetd_pid
```

---

**Note:** On a Hewlett-Packard UNIX platform, use `inetd -c` to send a `SIGHUP` to `inetd`.

---

- On Windows servers, do the following:
  - Verify that the `bpcd` entries are correct in the following:

```
%SystemRoot%\system32\drivers\etc\services
```

- Verify that the following numbers match the settings in the `services` file:  
**NetBackup Client Service Port** number and **NetBackup Request Service Port** number on the **Network** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and select **NetBackup Client Properties** on the **File** menu.  
The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.
- Stop and restart the NetBackup services.
- Perform the following procedures:  
See "Testing the media server and clients" in the [NetBackup Troubleshooting Guide](#).  
See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- If necessary, create debug log directories for `bprd` and retry the operation. Then, check the resulting debug logs on the master server:
  - If the error occurred during a backup operation, check the `nbpem`, `nbjm`, and `nbrb` logs by using the `vxlogview` command.
  - If the error occurred during a restore operation, check the `bprd` debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 205

**Message:** cannot connect to server backup restore manager

**Explanation:** A process on the master server cannot connect to a process on a host on the network. This error occurs when the process tries to initiate communication with the server that has the storage unit. This problem can occur during a backup or restore in either a single or a multiple server configuration.

**Recommended Action:** Run the `ping` command from one host to another by using the following combinations:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
- From each of the media servers, ping the master server by using the name that is specified in the NetBackup server list. On a UNIX or Linux server, this master is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box. See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

- On a UNIX or Linux server, verify that the `bpcd` entry in `/etc/services` or NIS on all the servers are identical. Verify that the media host listens on the correct port for connections to `bpcd`. To verify, run one of the following commands (depending on platform and operating system):

```
netstat -a | grep bpcd
```

```
netstat -a | grep 13782 (or the value that is specified during the install)
```

```
rpcinfo -p | grep 13782 (or the value that is specified during the install)
```

- On Windows servers, do the following:
  - Verify that the `bpcd` entries are correct in the services file:
 

```
%SystemRoot%\system32\drivers\etc\services
```
  - Verify that the following numbers match the settings in the `services` file:
 **NetBackup Client Service Port** number and **NetBackup Request Service Port** number on the **Network** tab in the **NetBackup Client Properties** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and select **NetBackup Client Properties** on the **File** menu. The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.
  - Stop and restart the NetBackup services.
- Perform the following procedures:
  - See "Testing the media server and clients" in the [NetBackup Troubleshooting Guide](#).
  - See "Resolving network communication problems" in the [NetBackup Troubleshooting Guide](#).
- Create a `bpcd` debug log directory on the server that has the storage unit and retry the operation. Then, check for additional information in the debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 206

**Message:** access to server backup restore manager denied

**Explanation:** The master server tries to start a process on another server (or itself) but does not appear in the NetBackup server list on that server. On a UNIX or Linux server, the master is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box.



See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).

**Recommended Action:** Do the following, as appropriate:

- Verify that the master server appears as a server in its own server list as well as being listed on all media servers.  
If you change the master server list, stop and restart the NetBackup Database Manager (bpdbm) and NetBackup Request Daemon (bprd) to ensure that all appropriate NetBackup processes use the new server entry.
- If necessary, create debug log directories for bprd and retry the operation. Then, check the resulting debug logs on the master server:
  - If the error occurred during a backup operation, check the nbpem, nbjm, and nbrb logs by using the vxlogview command.
  - If the error occurred during a restore operation, check the bprd debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 207

**Message:** error obtaining date of last backup for client

**Explanation:** When nbpem tries to obtain the date of the last backup for a particular client, policy, and schedule combination, an error occurs.

**Recommended Action:** Do the following, as appropriate:

- Verify that the NetBackup Database Manager (bpdbm) process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) is running.
- Examine the All Log Entries report for the appropriate time frame to gather more information about the failure.
- For detailed troubleshooting information, create a bpdbm log directory on the master server. Increase the logging level for the diagnostic and debug logs for nbpem.

Use the vxlogcfg command as explained in the following topic:

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

Retry the operation, then check the resulting logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 209

**Message:** error creating or getting message queue

**Explanation:** When a NetBackup process tries to create an internal message queue construct for inter-process communication, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the `bprd` debug log.

On UNIX and Linux servers, also gather the output of the `ipcs -a` command to see what system resources are currently in use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 210

**Message:** error receiving information on message queue

**Explanation:** When a NetBackup process tries to receive a message from a NetBackup daemon using `bprd` on an internal message queue construct, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the `bprd` debug log.

On UNIX and Linux servers, also gather the output of the `ipcs -a` command to see what system resources are currently in use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 212

**Message:** error sending information on message queue

**Explanation:** When a NetBackup process tries to attach to an already existing internal message queue construct for inter-process communication, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the `bprd` debug log.

On UNIX and Linux servers, also, gather the output of the `ipcs -a` command to see what system resources are currently in use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 213

**Message:** no storage units available for use

**Explanation:** The NetBackup resource broker (`nbrb`) did not find any storage units available for use. Either all storage units are unavailable or all storage units are configured for **On demand only**. In addition, the policy and schedule does not require a specific storage unit.

**Recommended Action:** Do the following, as appropriate:

- Examine the Backup Status and All Log Entries report for the appropriate time period to determine the policy or schedule that received the error.
- Verify that the media server has not been deactivated for the storage unit or units that are unavailable.
- Verify that the storage unit's drives are not down.
- Verify the following attribute settings for all storage units:
  - For disk storage units, the **Maximum concurrent jobs** is not set to 0
  - For Media Manager storage units, the **Maximum concurrent write drives** is not set to 0
- Verify that the robot number and host name in the storage unit configuration matches the Media and Device Management device configuration.
- Determine if all storage units are set to **On demand only** for a combined policy and schedule that does not require a specific storage unit. In this case, either specify a storage unit for the policy and the schedule combination or turn off **On demand only** for a storage unit.
- If the storage unit is on a UNIX or Linux NetBackup media server, it may indicate a problem with `bpcd`. Check `/etc/inetd.conf` on the media server to verify that the `bpcd` entry is correct.

If the storage unit is on a Windows NetBackup media server, verify that the NetBackup Client service was started on the Windows NetBackup media server.

- For detailed troubleshooting information, increase the logging levels of `nbrb` and `mds` on the master server.  
 Use the `vxlogcfg` command as explained in the following topic:  
 See "About unified logging" in the [NetBackup Logging Reference Guide](#).  
 Retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 215

**Message:** failed reading global config database information

**Explanation:** During the periodic checking of the NetBackup configuration, `nbproxy` was unable to read the global configuration parameters.

**Recommended Action:** Do the following, as appropriate:

- On UNIX and Linux master servers, verify that the NetBackup Database Manager (`bpdbm`) process is running. On a Windows master server, verify that the NetBackup Database Manager service is running.
- Try to view the global configuration settings by using the NetBackup administration interface (on UNIX and Linux systems), or by using Host Properties (on Windows systems).
- For detailed troubleshooting information, create debug log directories for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs for these processes. Also check the `nbpem` logs by using the `vxlogview` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 216

**Message:** failed reading retention database information

**Explanation:** During its periodic checking of the NetBackup configuration, `nbpem` did not read the list of retention levels and values.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux master server, verify that the NetBackup Database Manager (`bpdbm`) process is running. On a Windows master server, verify that the NetBackup Database Manager service is running.
- For detailed troubleshooting information, create a debug log directory for `bpdbm` on the master server.

Increase the logging level for `nbpem` by using the `vxlogcfg` command as described in the following topic:

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

Retry the operation and check the resulting logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 217

**Message:** failed reading storage unit database information

**Explanation:** During its periodic checking of the NetBackup configuration, `nbpem` did not read the storage unit configuration.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux server, verify that the NetBackup Database Manager (`bpdbm`) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.
- Try to view the storage unit configuration by using the NetBackup administration interface.
- For detailed troubleshooting information, create debug logs for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs. Also check the `nbpem` logs by using the `vxlogview` command.

Ensure that the correct master server is specified for the connection.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 218

**Message:** failed reading policy database information

**Explanation:** During the periodic checking of the NetBackup configuration, `nbpem` did not read the backup policy configuration.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux server, verify that the NetBackup Database Manager (`bpdbm`) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.
- Try to view the policy configuration by using the NetBackup administration interface.

- For detailed troubleshooting information, create debug log directories for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs. Also check the `nbpem` logs by using the `vxlogview` command. Ensure that the correct master server is specified for the connection.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 219

**Message:** the required storage unit is unavailable

**Explanation:** The policy or schedule for the backup requires a specific storage unit, which is currently unavailable. This error also occurs for other tries to use the storage unit within the current backup session.

**Recommended Action:** Look in the Job Details window for the failed job.

- Verify that the schedule specifies the correct storage unit and the storage unit exists.
- Verify that the following devices are running: the Media Manager device daemon (`ltid`) (UNIX or Linux server) or the NetBackup Device Manager service (Windows server). Use `bpps` on UNIX and Linux and the Activity Monitor on Windows or the Services application in the Windows Control Panel.
- Verify the following attribute settings:
  - For a disk storage unit, **Maximum concurrent jobs** is not set to 0.
  - For a Media Manager storage unit, the **Maximum concurrent drives** attribute is not set to 0.
- If the storage unit is a tape, verify that at least one of the drives is in the UP state. Use the Device Monitor.
- Verify that the robot number and host in the storage unit configuration match what is specified in the Media and Device Management device configuration.
- Verify that the master server can communicate with the `bpcd` process on the server that has the storage unit.

- Verify that `bpcd` listens on the port for connections.

On a UNIX or Linux server where the storage unit is connected, if you run `netstat -a | grep bpcd`, it should return something similar to the following:

```
*.bpcd *.* 0 0 0 0 LISTEN
```

On a Windows NetBackup server where the storage unit is connected, run `netstat -a` to print several lines of output. If `bpcd` listens, one of those lines is similar to the following:

```
TCP      myhost:bpcd                0.0.0.0:0                LISTENING
```

- Check the `nbrb` and the `mds` logs by using the `vxlogview` command.
- If the cause of the problem is not obvious, perform some of the steps in the following procedure:  
See Resolving Network Communication Problems in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 220

**Message:** database system error

**Explanation:** The `bpdbm` process (UNIX and Linux), or the NetBackup Database Manager service (Windows) did not create a directory path for its configuration catalogs. This error is due to a system call failure, which is usually due to a permission problem or an out of space condition.

**Recommended Action:** Create a debug log directory for `bpdbm`. Increase the logging level for the diagnostic and debug logs for `nbemm`.

Use the `vxlogcfg` command as explained in the following topic:

See "About unified logging" in the [NetBackup Logging Reference Guide](#).

Retry the operation and check the resulting logs for information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 221

**Message:** continue

**Explanation:** This status code is used to coordinate communication between various NetBackup processes and normally does not occur. If the logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

**Recommended Action:** Determine the cause of the status code that follows this one.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 222

**Message:** done

**Explanation:** This status code is used to coordinate communication between various NetBackup processes and is normally not seen. If the error logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

**Recommended Action:** Determine the cause of the status code that follows this one.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 223

**Message:** an invalid entry was encountered

**Explanation:** A request to the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) had invalid information or some information that conflicted. This error is usually a result of the use of software from different versions. Another cause can be incorrect parameters on a command.

**Recommended Action:** Verify that all NetBackup software is at the same version level and the command parameters are specified correctly. If neither of these is the problem, obtain detailed troubleshooting information by creating a `bpdbm` debug log directory. Then retry the operation. Check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 224

**Message:** there was a conflicting specification

**Explanation:** A request to the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) had some information that conflicted. This error is usually a result of the use of software from different version levels together.

**Recommended Action:** Verify that all NetBackup software is at the same version level. If that is not the problem, obtain detailed troubleshooting information by



creating `bpdbm` and `admin` debug log directories. Then retry the operation. Check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 225

**Message:** text exceeded allowed length

**Explanation:** Text in a request exceeds a buffer size. The request was made to the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows). This error is usually a result of the use of software from different version levels.

**Recommended Action:** Verify that all NetBackup software is at the same version level. If that is not the problem, create debug log directories for `bpdbm` and `admin`. Then, retry the operation and examine the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 226

**Message:** the entity already exists

**Explanation:** The configuration already has an entity with the same name or definition. For example: this status appears if you add a new policy when an existing policy has the same name or definition such as attributes or clients.

**Recommended Action:** Correct your request and re-execute the command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 227

**Message:** no entity was found

**Explanation:** The item requested was not in the catalog. For example, the entity can be a file or it can be policy information.

**Recommended Action:** A query may have no matching images. Specify different parameters or options for the operation and try the query again.

To restore selected files from a virtual machine to the original location, you must specify the host name of the virtual machine. Do not specify the display name or UUID as the destination.

More information is available about this message:

<http://www.veritas.com/docs/TECH208764>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 228

**Message:** unable to process request

**Explanation:** An inconsistency exists in the catalog or a request was made that would be improper to satisfy.

**Recommended Action:** Do the following, as appropriate:

- If this status involves a media server, verify that its server list specifies the correct master server. On a UNIX or Linux server, the master server is the first `SERVER` entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box.  
See "Using the Host Properties window to access configuration settings" in the [NetBackup Troubleshooting Guide](#).
- For detailed troubleshooting information, create a `bpdbm` debug log directory and retry the operation. Then, check the resulting debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 229

**Message:** events out of sequence - image inconsistency

**Explanation:** A request was made that can cause the image catalog to become inconsistent if satisfied

**Recommended Action:** Obtain detailed troubleshooting information by creating a debug log directory for `bpdbm`. Then, retry the operation, save the resulting debug log, and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 230

**Message:** the specified policy does not exist in the configuration database

**Explanation:** The specified policy name does not exist.

**Recommended Action:** Correct your parameters or options and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 231

**Message:** schedule windows overlap

**Explanation:** The specified start and the duration times for one day of the schedule overlap with another day of the schedule.

**Recommended Action:** Correct the schedule to eliminate the overlapping backup windows.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 232

**Message:** a protocol error has occurred

**Explanation:** This error is an intermediate status code that usually precedes another status code. It indicates the following: either the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) or the process that communicates with it has received unexpected information.

**Recommended Action:** Create a debug log directory for `bpdbm`. Then, retry the operation, save the debug log, and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 233

**Message:** premature eof encountered

**Explanation:** This status code is an intermediate one that usually precedes another status code and is associated with a problem in network communication.

**Recommended Action:** During a restore, this status code means that `tar` (on the client) received a stream of data that was not what it expected. If the restore is a new configuration, verify that the tape drive is configured for variable mode.

See the [NetBackup Device Configuration Guide](#).

If the communication failure is not due to an interrupt on a client system, save all error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 234

**Message:** communication interrupted

**Explanation:** This status code is an intermediate one that usually precedes another status code and is associated with a problem in network communication. Either a server or a client process received an interrupt signal.

**Recommended Action:** Save all error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 235

**Message:** inadequate buffer space

**Explanation:** This code usually indicates a mismatch between server and client software versions.

**Recommended Action:** Do the following, as appropriate:

- Verify that all NetBackup software is at the same version level. Update earlier versions of NetBackup software.
  - On UNIX and Linux, NetBackup servers and clients, check the `/usr/opensv/netbackup/bin/version` file.
  - On Windows NetBackup servers, check the `install_path\NetBackup\version.txt` file or the **About NetBackup** item on the **Help** menu.
  - On Microsoft Windows clients, check the **About NetBackup** item on the **Help** menu.
- If the problem persists, save all error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 236

**Message:** the specified client does not exist in an active policy within the configuration database

**Explanation:** A client name was not specified or the specified client does not exist.

**Recommended Action:** Activate the required policy, correct the client name, or add the client to a policy that meets your needs. After you make the correction, retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 237

**Message:** the specified schedule does not exist in an active policy in the configuration database

**Explanation:** The specified schedule does not exist in the NetBackup configuration.

**Recommended Action:** Activate the required policy, correct the schedule name, or create a schedule in a policy that meets your needs. After you make the correction, retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 238

**Message:** the database contains conflicting or erroneous entries

**Explanation:** The catalog has an inconsistent or a corrupted entry.

**Recommended Action:** Obtain detailed troubleshooting information for `bpdbm` (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) by creating a debug log directory for it. Then, retry the operation, save the resulting debug log, and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 239

**Message:** the specified client does not exist in the specified policy

**Explanation:** The specified client is not a member of the specified policy.

**Recommended Action:** Correct the client name specification, specify a different policy, or add the required client name to the policy. After you make the correction, retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 240

**Message:** no schedules of the correct type exist in this policy

**Explanation:** The appropriate schedule was not found in the specified policy. For example, a user backup specified a policy name but no user backup schedule exists in that policy.

**Recommended Action:** Specify a different policy or create a schedule of the needed type in the policy. After you make the correction, retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 241

**Message:** the specified schedule is the wrong type for this request

**Explanation:** The specified schedule for an immediate manual backup is not for a full nor an incremental backup. It must be one of these.

**Recommended Action:** Specify only full or incremental schedules for manual backups. If one does not exist in the policy, create one.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 242

**Message:** operation would cause an illegal duplication

**Explanation:** If the request is processed, it causes a duplicate entry (for example, in the catalog or the configuration database). A duplicate catalog entry is usually due to a mistake in the specification of media IDs for NetBackup catalog backups.

**Recommended Action:** Check the error reports to determine the specific duplication that would occur. Correct the settings for the operation and retry it.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 243

**Message:** the client is not in the configuration

**Explanation:** The specified client name was not in the catalog.

**Recommended Action:** Either correct the client name or add the client to the wanted policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 245

**Message:** the specified policy is not of the correct client type

**Explanation:** A user backup specified a policy that is not the type that is required for the client.

**Recommended Action:** Retry the operation by specifying a policy that is the correct type for the client. If such a policy does not exist, create one.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 246

**Message:** no active policies in the configuration database are of the correct client type

**Explanation:** A user backup request was not satisfied because no active policies were the type that were required for the client.

**Recommended Action:** Create or activate an appropriate policy so the user backup request can be satisfied.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 247

**Message:** the specified policy is not active

**Explanation:** Backups for the specified policy are disabled because the policy is inactive.

**Recommended Action:** Activate the policy and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 248

**Message:** there are no active policies in the configuration database

**Explanation:** No active policy was found that would satisfy the request.

**Recommended Action:** Activate the appropriate policy and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 249

**Message:** the file list is incomplete

**Explanation:** While the server waited for the client to finish sending the file list, it timed out or a sequencing problem occurred.

**Recommended Action:** First, obtain additional information by creating debug logs. Then try to recreate the error. The debug logs to create are as follows:

- On the server, `bptm`, `bpbrm`, and `bpdbm`.
- On UNIX, Linux, and Windows clients, `bpbkar`.
- On other clients, `bpcd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 250

**Message:** the image was not created with TIR information

**Explanation:** This error is internal and should not appear to customers.

**Recommended Action:** Obtain detailed troubleshooting information by creating debug logs for `bptm` or `bpdbm` on the server. Then, retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 251

**Message:** the tir information is zero length

**Explanation:** For a true-image backup, the client sent no file information to the master server. NetBackup discovered this condition when it tried to write the TIR information to media.

**Recommended Action:** Check the policy file list and the exclude and include lists on the client to verify that the client has eligible files for backup. For example, this status code can appear if the exclude list on the client excludes all files.

To obtain detailed troubleshooting information, create debug logs for `bptm` or `bpdbm` on the server. Then, retry the operation and check the resulting debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 252

**Message:** An extended error status has been encountered, check detailed status

**Explanation:** If a process was unable to report the extended error status as the final job status, the job exits with status 252. (The extended error status has a number greater than 255.)

**Recommended Action:** To determine the actual error, examine the job details display.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 253

**Message:** the catalog image .f file has been archived

**Explanation:** The catalog image .f file was archived.

**Recommended Action:** Refer to the catalog archiving help information to restore the archived catalog image .f files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 254

**Message:** server name not found in the NetBackup configuration

**Explanation:** This error should not occur through the normal use of NetBackup.

**Recommended Action:** Save all of the error information and contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 256

**Message:** logic error encountered

**Explanation:** An internal Vault error occurred.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 257

**Message:** failed to get job data

**Explanation:** This error can indicate either of the following:

- Vault failed to get job data because of a broken connection with the Job Manager (nbjm).
- Vault received empty job data. This error occurs if a user-specified job ID on the `vltrun -halttdups` command is out of range. (That is, the job ID is not among the job IDs created by Job Manager.)

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 258

**Message:** Vault duplication was aborted by administrator request

**Explanation:** The administrator initiated an abort request on the active vault duplication job.

**Recommended Action:** Ensure that the abort request was intentional.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 259

**Message:** vault configuration file not found

**Explanation:** This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 260

**Message:** failed to send signal

**Explanation:** vltrun failed to send a signal to the Vault duplication job.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 261

**Message:** vault internal error 261

**Explanation:** This error code should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 262

**Message:** vault internal error 262

**Explanation:** This error code should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 263

**Message:** session ID assignment failed

**Explanation:** The unique identifier to be assigned to the Vault session is corrupt.

**Recommended Action:** Verify that the session ID that is stored in the `session.last` file is valid.

UNIX and Linux:

```
/usr/openv/netbackup/vault/sessions/vault_name/session.last
```

Windows:

```
install_path\Netbackup\vault\sessions\vault_name\session.last
```

Make sure that the file system is not full and that no one has inadvertently edited the `session.last` file. To correct the problem, store the highest session ID that was assigned to a session for this Vault in the `session.last` file. If the problem persists, contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 265

**Message:** session ID file is empty or corrupt

**Explanation:** The session ID that is stored in the following file is corrupt.

UNIX and Linux:

```
/usr/openv/netbackup/vault/sessions/vault_name/session.l  
ast
```

Windows:

```
install_path\NetBackup\vault\sessions\vault_name\session  
.last
```

**Recommended Action:** Ensure that the session ID that is stored in the `session.last` file is not corrupt. Make sure that the file system is not full and that no one has inadvertently edited the file. To correct the problem, store the highest session ID that was assigned to a session for this Vault in the `session.last` file. If the problem persists, contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 266

**Message:** cannot find robot, vault, or profile in the vault configuration

**Explanation:** NetBackup cannot find the specified *profile\_name* or triplet *robot\_name/vault\_name/profile\_name* on the Vault command (`vltrun`, `vlteject`, `vltoffsitemedia`) or in `vltopmenu` in the Vault configuration.

**Recommended Action:** Rerun the command with the correct *profile\_name* or triplet *robot\_name/vault\_name/profile\_name*.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 267

**Message:** cannot find the local host name

**Explanation:** A Vault job obtains the local host name through an OS call. This error occurs when the Vault job is unable to get the local host name.

**Recommended Action:** Issue a `hostname` command at the OS command prompt. See the `hostname` (or `gethostbyname`) man page for an explanation of the conditions that would cause it to fail.

See the [OS System Administrator's Guide](#) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 268

**Message:** the vault session directory is either missing or inaccessible

**Explanation:** This error occurs when a Vault job cannot access the following:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions`

Windows: `install_path\NetBackup\vault\sessions`

This directory is created when Vault is installed.

**Recommended Action:** Make sure that you are running on the master server where Vault is installed and configured. Also ensure that no one accidentally removed the sessions directory or changed permission on the directory path so it is inaccessible to the Vault job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 269

**Message:** no vault session ID was found

**Explanation:** This error is encountered when `vltopmenu` cannot find a `sidxxx session id` directory for the specified profile. Either no Vault jobs were run for this profile or the corresponding `sidxxx session id` directory (or directories) were removed from the following directory:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions/vault_name`

Windows: `install_path\NetBackup\vault\sessions\vault_name`

**Recommended Action:** Either specify a different profile for the Vault jobs that were run or exit `vltopmenu` and run a Vault job for the specific profile. Then rerun `vltopmenu` and select the profile.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 270

**Message:** unable to obtain process id, getpid failed

**Explanation:** This error occurs when a Vault process is unable to obtain its process ID by means of the `getpid()` OS system call.

**Recommended Action:** Look at the system log for any unusual system problems. Wait a while and then try running the process again when system resources are freed up.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 271

**Message:** vault XML version mismatch

**Explanation:** The Vault upgrade process failed.

**Recommended Action:** Enable logging, start `nbvault`, and then examine the `nbvault` logs to determine the cause of the failure. If the upgrade process fails again, contact your customer support representative.

The following are the locations of the `nbvault` logs:

UNIX and Linux: `/usr/opensv/netbackup/logs/nbvault/`

Windows: `install_path\NetBackup\logs\nbvault`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 272

**Message:** execution of a vault notify script failed

**Explanation:** This error occurs when the Vault process is unable to run a Vault notify script due to permissions problems or coding problems in the script. It also occurs if the script returns an error.

**Recommended Action:** Ensure that the notify script is executable and runs without errors. You must debug the script by running it manually to eliminate coding errors.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 273

**Message:** invalid job id

**Explanation:** This error can occur in either of the following situations:

- The specified job is not an active Vault job
- The specified active Vault job is not at the duplication step

**Recommended Action:** Specify the job ID of the active Vault job that is currently at the duplication step or operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 274

**Message:** no profile was specified

**Explanation:** This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 275

**Message:** a session is already running for this vault

**Explanation:** This error occurs when you start a session for a vault and another session is already running for this vault. Only one session is allowed for a vault at any given time.

**Recommended Action:** Start the Vault session after the previous session has completed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 276

**Message:** invalid session ID

**Explanation:** This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 277

**Message:** unable to print reports

**Explanation:** This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 278

**Message:** unable to collect pre eject information from the API

**Explanation:** This error occurs when robotic information cannot be retrieved before ejection.

**Recommended Action:** Ensure that all Media and Device Management daemons are running or the robot is live and up.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 279

**Message:** eject process is complete

**Explanation:** This error occurs when the eject process is completed successfully.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 280

**Message:** there are no volumes to eject

**Explanation:** This error occurs when media to be ejected are not in the library.

**Recommended Action:** Ensure that the media to be ejected are not removed from the library manually.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 281

**Message:** vault core error

**Explanation:** An internal Vault error occurred.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 282

**Message:** cannot connect to nbvault server

**Explanation:** The vault job cannot connect to the NetBackup Vault Manager service (nbvault on UNIX and Linux, nbvault.exe on Windows).

Possible causes are the following:

- The &CompanyName; Private Branch Exchange service (VRTSspbxx) or NetBackup Request Manager (bprd) is down.
- The NetBackup Vault Manager service is down, possibly because of the following: the Vault is not licensed, the vault.xml configuration file is corrupt, or the vault.xml configuration file upgrade failed during an upgrade installation.

**Recommended Action:** To determine the reason for failure, examine the logs for the service or services that are down and the operating system logs (EventLog on Windows). Restart the service or services that are down after resolving the problem.

The following are the locations of the nbvault logs:

UNIX and Linux: /usr/opensv/netbackup/logs/nbvault/

Windows: install\_path\NetBackup\logs\nbvault

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 283

**Message:** error(s) occurred during vault report generation

**Explanation:** Vault encountered errors during the report generation phase.

**Recommended Action:** Check logs for details of the failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 284

**Message:** error(s) occurred during vault report distribution

**Explanation:** Vault encountered errors during the report distribution phase. Potential reasons include the following:

- Reports were not emailed (possibly because of malformed email addresses in the vault.xml file).
- On Windows, the third-party mail client (such as blat) is not configured properly.

- The reports destination directory is not present or it does not have appropriate permissions.
- The printer is not set up correctly or the printer command in `vault.xml` is incorrect.

**Recommended Action:** Check logs for details of the failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 285

**Message:** unable to locate vault directory

**Explanation:** A Vault job or a command for a missing or a corrupt directory of the session in question returns this error.

**Recommended Action:** The `vault` directory is created when the Vault package is installed on the master server. Ensure that the Vault job or command is started as root on the master server. Ensure that the `vault` directory was not removed inadvertently or made inaccessible to the root user.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 286

**Message:** vault internal error

**Explanation:** This error should never occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 287

**Message:** vault eject failed

**Explanation:** This error occurs when Vault fails to eject any of the media that was identified for eject during a Vault Session. Potential reasons: Media and Device Management services are down, the robot is down, or no empty slots are available in the media access port (MAP).

**Recommended Action:** Ensure that the Media and Device Management services are running, the robot is up, and empty slots are available in the media access port (MAP).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 288

**Message:** vault eject partially succeeded

**Explanation:** This error occurs when not all of the media that was identified for eject during a Vault session can be ejected.

Potential reasons include the following:

- Some of the media is in use by NetBackup
- Some of the media are in a drive
- Not enough empty slots are available in the media access port (MAP)

**Recommended Action:** Ensure that the media are not loaded in a drive and in use by other processes. Ensure that empty slots are available in the media access port (MAP).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 289

**Message:** cannot consolidate reports of sessions from container and slot-based vaults

**Explanation:** This error occurs when you consolidate reports and at least one session uses slots and another uses containers.

**Recommended Action:** Change the report consolidation so that only reports for one type of vault operation are consolidated, either slots or containers.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 290

**Message:** one or more errors detected during eject processing

**Explanation:** This error occurs when more than one error is encountered during an eject procedure by `vltopmenu`. Any "eject" errors that range from 291 to 300 may have occurred in any of the sessions being ejected.

**Recommended Action:** For detailed information, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

After the problem is identified and corrected, the media that were not ejected may need to be ejected manually by means of `vlteject` or `vltopmenu`.

This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP.

To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robotic library.
- Inventory the robotic library. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then rerun the Vault sessions that failed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 291

**Message:** number of media has exceeded capacity of MAP; must perform manual eject using `vltopmenu` or `vlteject`

**Explanation:** This error occurs in the following situation: a Vault job is run for a profile that selected automatic eject mode and the number of media to be ejected exceeds the MAP capacity.

**Recommended Action:** Use `vltopmenu` to manually eject the media for the selected profile and session ID. The `vltopmenu` option lets you eject the selected media, a MAP-full (or less) at a time.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 292

**Message:** eject process failed to start

**Explanation:** This error occurs when the following cannot start the eject process: the Vault job, the `vlteject` command, or the use of the `vltopmenu`.

**Recommended Action:** For detailed information about the problem, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

Use the `robtest` utility to ensure that you can communicate with the Vault robotic library. After the problem is resolved, rerun the Vault session, `vlteject` command, or `vltopmenu` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 293

**Message:** eject process has been aborted

**Explanation:** This error occurs when the eject process is canceled. This error can be encountered during a Vault job or with the `vlteject` or the `vltopmenu eject` command.

This error can occur because of one of the following conditions:

- Could not open a pipe to `vmchange -verify_eject` call.
- Unexpected output from `vmchange -verify_eject` call.
- No MAP elements exist to eject media into.
- The robotic library had problems putting media into the MAP.
- The user pressed Return in interactive mode and did not first remove the media from the MAP. In this case, the media that were in the MAP are put back into their original slots in the robotic library.

**Recommended Action:** For detailed information about why the process was canceled, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux:

```
/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx
```

Windows:

```
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```

(where `xxx` is the session ID)

This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP.

To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robotic library.
- Inventory the robotic library. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then, rerun the Vault sessions that failed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 294

**Message:** vault catalog backup failed

**Explanation:** During a Vault job, the catalog backup step failed.

**Recommended Action:** Review the Vault debug log in the following directory for detailed information about why the process failed:

UNIX and Linux: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

To find the actual problem that caused the catalog backup (`bpbackupdb`) to fail, review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

Correct the problem and rerun the Vault job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 295

**Message:** eject process could not obtain information about the robot

**Explanation:** This error occurs when the eject process cannot collect information about the robotic library and its associated MAPs and volumes.

**Recommended Action:** For detailed information about why the process fails, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

Correct the error and rerun the Vault session, `vlteject` command, or `vltopmenu` eject command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 296

**Message:** process called but nothing to do

**Explanation:** This error occurs in the following situations:

- `vlteject` is called with `-eject` but the system has no tapes to eject
- `vlteject` is called with `-eject` and the eject is already done
- `vlteject` is called with `-report` and the reports are already done
- `vlteject` is called with `-eject` and `-report`, and both the eject and the reports are done

**Recommended Action:** This error is an informative one and does not require any action.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 297

**Message:** all volumes are not available to eject

**Explanation:** This error occurs when a try is made to eject a non-existent or bad media ID during the eject phase of the following: a Vault session, a `vlteject` command, or a `vltopmenu` command.

Possible reasons for this error are as follows:

- The bad media ID was added by means of the `vltejectlist_notify` script.
- The bad media ID is already in the MAP or not in the robotic library.
- The bad media ID is in a robotic drive.
- The bad media ID is in transit in the robotic library.

**Recommended Action:** Remove or correct the defective media ID from the `vltejectlist_notify` script and rerun the Vault session. If the bad media ID is in the MAP or a drive or in transit, something is misconfigured.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 298

**Message:** the library is not ready to eject volumes

**Explanation:** This error occurs if the robotic library is not in a state to support ejecting media.

Possible reasons for this error include the following:

- Currently, the library ejects media
- The library waits to eject media
- Currently, the library injects media
- The library waits to inject media

**Recommended Action:** Wait until the robotic library can support the eject action and rerun the Vault session, `vlteject` command, or `vltopmenu` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 299

**Message:** there is no available MAP for ejecting

**Explanation:** The robotic library you vault from does not have a MAP available for use and so media cannot be ejected.



**Recommended Action:** Wait until the robotic library's MAP is available for use and rerun the Vault session, `vlteject` command, or `vltopmenu` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 300

**Message:** vmchange eject verify not responding

**Explanation:** During the eject process, the `vmchange` command is called with a `-verify_eject` call until all of the volumes for the request are in the MAP. This command call failed. Or it did not return the proper information to the Vault eject process.

**Recommended Action:** Do the following, as appropriate:

- Review the Vault debug log in the following directory for detailed information about why the process failed:

```
UNIX: /usr/opensv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault
```

- Also review the `summary.log` in each of the `sidxxx` directories that had problems:

```
UNIX:/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx
Windows:install_path\NetBackup\vault\sessions\vault_name\sidxxx
(where xxx is the session ID)
```

This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP. To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robot.
- Inventory the robot. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then, rerun the Vault sessions that failed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 301

**Message:** vmchange api\_eject command failed

**Explanation:** During the eject process, the `vmchange` command is called with an `-api_eject` call to begin the process to eject media. This command call failed.

**Recommended Action:** Review the Vault debug log in the following directory for detailed information about why the process failed:

UNIX: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

When the problem is resolved, rerun the Vault session, `vlteject` command, or `vltopmenu` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 302

**Message:** error encountered trying backup of catalog (multiple tape catalog backup)

**Explanation:** This error occurs when the NetBackup command that was used for stage one of the two-stage catalog backup fails.

**Recommended Action:** For the actual error that caused the failure, review the Vault debug log in the following directory:

UNIX: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

In addition, review the admin debug log in the following directory:

UNIX: `/usr/opensv/netbackup/logs/admin`

Windows: `install_path\NetBackup\logs\admin`

Correct the error and rerun the Vault session.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 303

**Message:** error encountered executing Media Manager command

**Explanation:** This error occurs when a Media and Device Management command fails during a Vault job.

**Recommended Action:** For the actual error that caused the command to fail, review the Vault debug log in the following directory:

UNIX: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX: `/usr/opensv/netbackup/vault/sessions/vault_name/sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

Try running the command (with the same arguments as in the log file) to see the actual error. Ensure that the Media and Device Management daemons are running. Also ensure that the robot is functional and you can communicate with it (for example, inventory the robot through the GUI).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 304

**Message:** specified profile not found

**Explanation:** This error occurs when the profile name that is specified on the Vault command is not defined in the Vault configuration.

**Recommended Action:** Rerun the Vault command with a profile name that is defined in the Vault configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 305

**Message:** multiple profiles exist

**Explanation:** This error may occur when duplicate profile names are defined in multiple Vault configurations and only the profile name is specified on the Vault command.

**Recommended Action:** Rerun the Vault command with the triplet *robot\_name/vault\_name/profile\_name*. The triplet uniquely identifies the profile in your Vault configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 306

**Message:** vault duplication partially succeeded

**Explanation:** This error occurs when all selected images are not duplicated successfully.

**Recommended Action:** Check the Vault and `induplicate` logs for cause of the failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 307

**Message:** eject process has already been run for the requested Vault session

**Explanation:** This error occurs when `vlteject` is run to eject media for a session ID for which media has already been ejected.

**Recommended Action:** Rerun `vlteject` for another session ID for which media has not been ejected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 308

**Message:** no images duplicated

**Explanation:** This error occurs when Vault failed to duplicate any images.

**Recommended Action:** For more information, review the Vault debug log in the following directory:

UNIX: `/usr/openv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX: `/usr/openv/netbackup/vault/sessions/<vault_name>sidxxx`

Windows: `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where *vault\_name* is the name of the vault, and *xxx* is the session ID)

Look for the log entry that gives the total number of images processed. A common cause of failure is a lack of resources, such as no more media available in the specified pools for duplication. Correct the problem and rerun the Vault job. Note that the NetBackup scheduler retries a Vault job that terminates with this error. Review the admin debug log for duplicate entries and the `bptm` debug log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 309

**Message:** report requested without eject being run

**Explanation:** This error occurs when a report is run that requires media to have been ejected first.

**Recommended Action:** Perform one of these actions:

- Rerun `vlteject` or `vltopmenu` to eject the media for the session before you generate the reports.
- Reconfigure the profile to allow the eject step to be performed when the next Vault session for this profile runs.
- Disable the report generation in the profile for the reports that require media to be ejected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 310

**Message:** Updating of Media Manager database failed

**Explanation:** This error occurs when Vault physically ejects tapes but fails to update the EMM database to reflect the eject operation. A typical reason for this failure is that EMM detected a mismatch between the media type and its volume group.

**Recommended Action:** To find the root cause of the error, review the Vault debug logs in the following directory:

UNIX: `/usr/opensv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

To fix the issue may involve making configuration changes.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 311

**Message:** Iron Mountain Report is already created for this session

**Explanation:** This error occurs when an Iron Mountain report has already been generated for the session.

**Recommended Action:** None. This report cannot be generated again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 312

**Message:** invalid container database entry

**Explanation:** NetBackup Vault found an invalid entry while it read the container database. Each container entry in the container database must follow the expected format. The container database exists in file cntrDB, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** To get the line number of an invalid record in the container database, read the log file under the directory `netbackup/logs/vault`. Be aware that a Vault log may not exist unless the directory `netbackup/logs/vault` existed before the error occurred. Open the container database file cntrDB and correct that invalid entry. Note that this error occurs every time Vault reads this entry in cntrDB until either this invalid entry is deleted or it is corrected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 313

**Message:** container does not exist in container database

**Explanation:** The specified container does not have an entry in the container database. The container database exists in file cntrDB, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Verify that you put some media into this container by using the `vltcontainers` command. Verify that you did not delete it by using the `vltcontainers -delete` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 314

**Message:** container database truncate operation failed

**Explanation:** An error occurs while truncating the container database. This error may occur during the modification or deletion of an entry from the container database. The container database exists in file cntrDB, which is located at *install\_path/netbackup/vault/sessions/cntrDB*.

**Recommended Action:** See the log file under the directory *netbackup/logs/vault* for more details. Be aware that a log file is not created unless the *netbackup/logs/vault* directory has already been created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 315

**Message:** failed appending to container database

**Explanation:** This error can occur while appending a container record to the container database. This error may occur with the addition, modification, or deletion of an entry from the container database. The container database exists in file cntrDB, which is located at *install\_path/netbackup/vault/sessions/cntrDB*.

**Recommended Action:** Read the relevant log file under the directory *install\_path/netbackup/logs/vault* for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 316

**Message:** container\_id is not unique in container database

**Explanation:** NetBackup Vault has found a previously-existing entry for this container ID in the container database while adding it to the container database. Each container record in the container database must have a unique container ID. Note that the container database exists in file cntrDB, which is located at *install\_path/netbackup/vault/sessions/cntrDB*.

**Recommended Action:** Verify that you have specified the correct container ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 317

**Message:** container database close operation failed

**Explanation:** This error occurs while closing the container database. This error may occur during the reading, addition, modification, or deletion of an entry from the container database. Note that the container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 318

**Message:** container database lock operation failed

**Explanation:** This error occurs while locking the container database. This error may occur during the addition, modification, or deletion of an entry from the container database. Note that the container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file not created.

If some other Vault operation uses the container database and locks it, wait until that operation completes and the container database is unlocked.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 319

**Message:** container database open operation failed

**Explanation:** This error occurs while opening the container database. This error may occur during the reading, addition, modification, or deletion of an entry from the container database. Note that the container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.



Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 320

**Message:** the specified container is not empty

**Explanation:** This error occurs if you try to delete a container from the container database, but the container still holds media. You can only delete empty containers.

**Recommended Action:** Verify that you have specified the correct container ID.

If you still want to delete this container from the container database, first empty it by doing either of the following:

- Inject all of the media that it contains into a robot.
- Clear the Vault container ID fields for these media from the EMM database by using `vmchange -vlt cid` with a value of `-`.

Try to delete the container again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 321

**Message:** container cannot hold any media from the specified robot

**Explanation:** This error occurs while trying to place media from an unexpected EMM database host into a container. All the media that are placed in a container should belong to the same EMM database host. For example, you have media from a robot that belongs to one EMM database host. Then you try to put this media into a container that already holds media from the robots that belong to a different EMM database host.

**Recommended Action:** Verify that you specified the correct container ID and media IDs. Read the relevant log file under the directory `install_path/netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 322

**Message:** cannot find vault in vault configuration file

**Explanation:** NetBackup Vault cannot find an entry for the specified Vault name into the Vault configuration file. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Verify that you specified the correct Vault name. Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 323

**Message:** cannot find robot in vault configuration file

**Explanation:** NetBackup Vault cannot find an entry for the specified robot number in the Vault configuration file. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Verify that you specified the correct robot number. Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 324

**Message:** invalid data found in retention map file for duplication

**Explanation:** This error occurs when the retention mapping file (either generic or for a specific vault) contains invalid data. If the file contains too much or too little data or the user defines invalid retention levels in the file, this error occurs.

The retention mapping file is used as follows: in a Vault session when a Vault profile duplication is configured with the Use mappings retention level configured for one of the copies for duplication. The product installs a mapping file template named `retention_mappings` in `install_path/netbackup/db/vault`.

To specify a mappings file for any single vault, copy the `retention_mappings` template to another file and append the name of the vault. For example,  
`netbackup/db/vault/retention_mappings.V1`

**Recommended Action:** Check the entries in the `retention_mappings` file.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 325

**Message:** unable to find policy/schedule for image using retention mapping

**Explanation:** This error occurs with duplication of the backup policy or the schedule of an image by Vault. The Use mappings option on the Duplication tab of the Profile dialog box is selected, but the policy or the schedule no longer exists.

**Recommended Action:** Verify whether or not the backup policy or the schedule that created the image still exists. If either one or both do not exist, the image is not duplicated through the Vault profile.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 326

**Message:** specified file contains no valid entry

**Explanation:** The specified file contains no valid entries for media IDs or the alphanumeric equivalent of barcodes. As per the expected format, each line should contain only one string that represents either a media ID or the barcode numeric equivalent.

**Recommended Action:** Verify that each entry in the specified file does not exceed the string size limit: six characters for media IDs and 16 characters for the numeric equivalent of barcodes. Correct the invalid entries in the specified file and try the same operation again. Read the relevant log file under the directory

`install_path/netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 327

**Message:** no media ejected for the specified vault session

**Explanation:** This error occurs while moving media ejected by the specified Vault session to a container. Either the specified Vault session has not ejected any media, or you specified an incorrect Vault name or session ID.

**Recommended Action:** Verify that you have specified the correct combination of Vault name and session ID. Verify that the specified Vault session has ejected at least one piece of media. Read the relevant log file under the directory

`netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 328

**Message:** invalid container ID

**Explanation:** This error occurs while adding a container record to the container database. The container ID is found invalid. Note that the container database exists in the `cntrDB` file that is located at

*install\_path/netbackup/vault/sessions/cntrDB.*

**Recommended Action:** Verify that the container ID does not contain any space characters, and that the string size is a maximum of 29 characters long.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 329

**Message:** invalid recall status

**Explanation:** This error occurs while adding a container record to the container database. The container recall status is found invalid. Note that the container database exists in the `cntrDB` file that is located at

*install\_path/netbackup/vault/sessions/cntrDB.*

**Recommended Action:** Verify that the recall status is either 1 or 0.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 330

**Message:** invalid database host

**Explanation:** This error occurs while adding a container record to the container database. The EMM database host name is found invalid. Note that the container database exists in the `cntrDB` file that is located at

*install\_path/netbackup/vault/sessions/cntrDB.*

**Recommended Action:** Verify that the EMM database host name does not contain any space characters, and that the string size is a maximum of 256 characters long.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 331

**Message:** invalid container description

**Explanation:** This error occurs while adding a container record to the container database. The container description is found invalid. Note that the container database exists in the `cntrDB` file that is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Verify that the string size of the container description is a maximum of 25 characters long.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 332

**Message:** error getting information from EMM database

**Explanation:** This error can occur while the backup process communicates with the EMM database to retrieve some information.

**Recommended Action:** Do the following, as appropriate:

- On UNIX, verify that the NetBackup Volume Manager (vmd) is running. On Windows, verify that the NetBackup Volume Manager service is running.
- See the process-specific error log directory for more details.

UNIX: `/usr/opensv/netbackup/logs/process_name`

Windows: `install_path\NetBackup\logs\process_name`

For example, if you get this error while running a Vault command (such as `vltcontainers` or `vltopmenu`), look at the following logs to learn why:

`/usr/opensv/netbackup/logs/vault`

---

**Note:** The log file cannot be created unless the appropriate log directory (for example, `/usr/opensv/netbackup/logs/vault`) is already created.

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 333

**Message:** error getting information from media manager command line

**Explanation:** This error occurs when Vault cannot retrieve robot information such as map information, volume information, library status, and so on. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 334

**Message:** unable to receive response from robot; robot not ready.

**Explanation:** This error occurs when a problem exists with the robot.

**Recommended Action:** Ensure that all Media and Device Management daemons are running or the robot is live and up.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 335

**Message:** failure occurred while suspending media for eject

**Explanation:** This error occurs when Vault cannot suspend the media. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 336

**Message:** failure occurred while updating session information

**Explanation:** Vault cannot update the session files. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 337

**Message:** failure occurred while updating the eject.mstr file

**Explanation:** Vault cannot update the eject list file. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 338

**Message:** vault eject timed out

**Explanation:** This error occurs when a problem exists with the robot.

**Recommended Action:** Do the following, as appropriate:

- Remove the media from the MAP if it is already full.
- Make sure that the MAP is closed properly.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 339

**Message:** vault configuration file format error

**Explanation:** The Vault configuration file is malformed. Unless the file has been manually modified, this error is internal. Note that the Vault configuration file is located at *install\_path/netbackup/db/vault/vault.xml*.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 340

**Message:** vault configuration tag not found

**Explanation:** An optional attribute may not appear in the Vault configuration file. This internal error generally does not cause problems in Vault's operation. Note that the Vault configuration file is located at *install\_path/netbackup/db/vault/vault.xml*.

**Recommended Action:** If the Vault's operation is affected, contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 341

**Message:** vault configuration serialization failed

**Explanation:** Vault failed to write out the Vault configuration file. It is an internal error. Note that the Vault configuration file is located at *install\_path/netbackup/db/vault/vault.xml*.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 342

**Message:** cannot modify - stale view

**Explanation:** This error can occur if an administration interface (**NetBackup Administration Console** or **Vault Administration** menu user interface) tries to modify the following:

- A robot or vault or profile in between the read
- Operations of the same robot or vault
- Profile by another instance of an administration interface

**Recommended Action:** Check the latest attributes of the robot or vault or profile. To check, refresh the view in the **NetBackup Administration Console** or retrieve the attributes in the **Vault Administration** menu user interface again. Then retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 343

**Message:** robot already exists

**Explanation:** This error can occur during addition of a robot while a robot with the same name already exists.

**Recommended Action:** Refresh the view in the **NetBackup Administration Console** or retrieve the attributes in the **Vault Administration** menu user interface again to see the robot.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 344

**Message:** vault already exists



**Explanation:** This error can occur during addition of a vault if a vault with the same name already exists in the same robot.

**Recommended Action:** Choose a different name for the vault.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 345

**Message:** profile already exists

**Explanation:** This error can occur during addition of a profile if a profile with the same name already exists within the same vault.

**Recommended Action:** Choose a different name for the profile.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 346

**Message:** duplicate MAP

**Explanation:** A duplicate MAP was added in the Vault configuration file. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 347

**Message:** vault configuration cache not initialized

**Explanation:** This error should never occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 348

**Message:** specified report does not exist

**Explanation:** An invalid Vault report was requested for generation. It is an internal error.

**Recommended Action:** Contact customer support and send the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 349

**Message:** incorrect catalog backup policy

**Explanation:** This error can occur when a Vault session tries to run a catalog backup. The specified policy for the catalog backup in the Vault profile is either blank or is not of type NBU-Catalog.

**Recommended Action:** Verify that you specified a catalog backup policy for the catalog backup in the Vault profile and that the policy is of type NBU-Catalog.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 350

**Message:** incorrect vault catalog backup schedule

**Explanation:** This error can occur when a Vault session tries to run a catalog backup. The specified Vault catalog backup schedule for catalog backup in the Vault profile is either blank or is not of type Vault Catalog Backup.

**Recommended Action:** Verify that you specified a Vault Catalog Backup schedule for the catalog backup in the Vault profile. Also verify that the schedule is of type Vault Catalog Backup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 351

**Message:** all configured vault steps failed

**Explanation:** This error occurs when multiple Vault steps are configured for a session and all of them fail.

**Recommended Action:** For duplication and catalog backup steps, use the Activity Monitor to check the status of the respective jobs that Vault started. For Eject step status, check the **Detailed Status** tab of the **Job Details** dialog box for the Vault job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 400

**Message:** Server Group Type is Invalid

**Explanation:** The creation of a server group fails because the server group type is invalid.

**Recommended Action:** Do the following, as appropriate:

- Select a valid server group type: MediaSharing, NetBackup OpsCenter, or AltServerRestore.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the logs for `nbemm` (originator ID 111) which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 401

**Message:** Server Group Already Exists

**Explanation:** The attempt to create a server group failed. The server group already exists.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified server group name is not in use.
- Create the server group by specifying a name that is not currently in use.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for `nbemm` (originator ID 111), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 402

**Message:** Server Group Already Exists with a different type

**Explanation:** The attempt to create a server group failed. The server group name is already in use by a server group with a different group type.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified server group name is not in use.

- Try to create the server group by specifying a name that is not currently in use.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 403

**Message:** Server Group Active State is not valid

**Explanation:** The attempt to create a server group failed. The server group state was invalid.

**Recommended Action:** Do the following, as appropriate:

- Valid server group states are: ACTIVE and INACTIVE
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 404

**Message:** Server Group does not exist

**Explanation:** An operation was tried by using a server group that does not exist.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified media is correct.
- Verify the media ownership.
- Verify that the server group exists.
- Verify that the server where the operation is performed is a member of the owning server group. If not, try the operation from a server that is a member of the server group.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 405

**Message:** Member's server type not compatible with Server Group

**Explanation:** The attempt to add or update a server group failed. A member's server type was not valid for the specified server group type.

**Recommended Action:** Do the following, as appropriate:

- The Media Sharing server group can contain the following types of servers: Master, Media, NDMP, and cluster.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 406

**Message:** The computer specified is not a member of the server group specified

**Explanation:** A server that is not a member of the server group that owns the media performed an operation on a media.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified media is correct.
- Verify the media ownership.
- Verify that the server where the operation is performed is a member of the owning server group. If not, try the operation from a server that is a member of the server group.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which use unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 407

**Message:** Member's NetBackup version not compatible with Server Group

**Explanation:** The attempt to add or update a server group failed. One of the server group member's NetBackup version is not valid for the specified server group type.

**Recommended Action:** Do the following, as appropriate:

- Ensure that each member server has a valid NetBackup version for the specified server group type.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for `nbemm` (originator IDs 111 and 143), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 408

**Message:** Server Group is in use

**Explanation:** The attempt to delete a server group that failed because the server group owns one or more media.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the server group is not the owner of any media by running `bpmedialist -owner group_name` from the master server.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for `nbemm` (originator IDs 111 and 143), which uses unified logging.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 409

**Message:** Member already exists in server group

**Explanation:** The attempt to add or update a server group failed because one of the server group members is the same as the one being added.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the server group member that you add does not already exist in the group.

- Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 501

**Message:** You are not authorized to use this application.

**Explanation:** The user is not authorized to use one of the NetBackup Java Administration utilities on the host that is specified in the login dialog box.

**Recommended Action:** Check the `auth.conf` file on the host that is specified in the NetBackup Java login dialog box for the proper authorization. If the `auth.conf` file does not exist, it must be created with the proper entry for this user name. More details on the `auth.conf` file are available.

See [NetBackup Administrator's Guide, Volume I](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 502

**Message:** No authorization entry exists in the `auth.conf` file for user name *username*. None of the NetBackup Java applications are available to you.

**Explanation:** The user name is not authorized to use any NetBackup Java applications on the host that is specified in the logon dialog box.

**Recommended Action:** Check the `auth.conf` file on the computer (host name) specified in the NetBackup Java logon dialog box for the proper authorization. If the file does not exist, create it with the proper entry for this user name. More details on the `auth.conf` file are available.

See [NetBackup Administrator's Guide, Volume I](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 503

**Message:** Invalid user name.

**Explanation:** For UNIX host logon, the NetBackup Java application server on the host where the logon is requested does not recognize the user name.

For Windows host logon, the NetBackup Java authentication service on the host where the logon is requested does not have sufficient privileges to grant the request.

**Recommended Action:** Do the following, as appropriate:

- For UNIX hosts: the user name must be a valid user name in the `passwd` file on the host that is specified in the logon dialog box.
- For Windows hosts: refer to the LogonUser function in the section titled Client/Server Access Control Functions of the *Windows Platform Software Developer's Kit* to determine the required privileges.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 504

**Message:** Incorrect password.

**Explanation:** For logon to a UNIX host, the user name is recognized on the host where the logon is requested, but the supplied password is incorrect.

For logon to a Windows host, the attempt to log in the user failed. The failure can be due to an unrecognized user in the specified domain.

**Recommended Action:** Do the following, as appropriate:

- Enter the correct password.
- On Windows hosts: The exact error can be found in the `bpjava-msvc` log file.

For more details, refer to the LogonUser function in the section Client/Server Access Control Functions of the *Windows Platform Software Developer's Kit*.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 505

**Message:** Cannot connect to the NetBackup Java authentication service on *host* on the configured port - (*port\_number*). Check the log file for more details.

**Explanation:** The initial connection from the NetBackup Java interface to its authentication service on (*host*) was on the configured `port_number` that was mentioned in the error message. Either the port is in use by another application or the NetBackup Java interface and its application server are not configured with the same port. The default port is 13722. The **NetBackup Administration Console** log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- On UNIX, compare the `bpjava-msvc` entry in the `/etc/services` file with the `BPJAVA_PORT` entry in the `/usr/opensv/java/nbj.conf` file



On Windows, compare the `bpjava-msvc` entry in the `%systemroot%\system32\drivers\etc\services` file with the `install_path\java\setconf.bat` file (Windows). The entries must match.

- Ensure that no other application uses the port that is configured for the NetBackup Java interface.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 506

**Message:** Cannot connect to the NetBackup Java user service on *host* on port *port\_number*. If successfully logged in before, retry your last operation. Check the log file for more details.

**Explanation:** After the NetBackup Java authentication service validates the user name, a NetBackup Java user service is used for all other service requests from the NetBackup Java interface. Communication was tried between the NetBackup Java interface and the user service on host (*host*) on the port number that was specified in the error message. More information about various port configuration options is available.

See [NetBackup Administrator's Guide, Volume I](#).

The **NetBackup Administration Console** log file should contain more detail about this error.

- On UNIX: the port configuration options are specified in the `/usr/opensv/netbackup/bp.conf` file or through the **NetBackup Administration Console Host Properties**.
- On Windows: from the **NetBackup Administration Console**, select **Host Properties**. Select **Properties** on the **Actions** menu. The **Port Ranges** tab contains the port options.

**Recommended Action:** Do the following, as appropriate:

- Restart the NetBackup Java interface and log in again.
- If the problem persists, enable detailed debug logging.
- Restart the NetBackup Java interface and examine the logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 507

**Message:** Socket connection to the NetBackup Java user service has been broken. Retry your last operation. Check the log file for more details.

**Explanation:** The connection was broken to the NetBackup Java application server that is running on the NetBackup host (where you are logged in). The **NetBackup Administration Console** log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- Retry the last operation.
- If the problem persists, restart the NetBackup Java interface and try again.
- If the problem still persists, enable detailed debug logging.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart the NetBackup Java interface and examine the logs.

---

**Note:** You may have network or system problems unrelated to NetBackup.

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 508

**Message:** Cannot write file.

**Explanation:** This cause of this error is one of the following:

- The NetBackup Java user service tries to write to a file that does not have write permissions. The solution is to enable write privileges.
- The NetBackup Java user service tries to write to a temporary file whose unique name cannot be constructed. This condition is unlikely, but can result from an exhaustion of system resources (from the filling of the name space).

**Recommended Action:** Retrieve the specific details from the user service log files.

Enable detailed debug logging as explained in the following topic:

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 509

**Message:** Cannot execute program.

**Explanation:** The NetBackup Java authentication or user service reported an error that relates to the creation (or demise) of a child job process. The NetBackup Java service programs create separate jobs to accomplish specific tasks, as follows. The NetBackup Java authentication service creates the NetBackup Java user service. When it is created and connected to, the NetBackup Java user service creates all other child processes on behalf of requests from the NetBackup Java interface.

The cause of status code 509 can be found in the appropriate log file, either for `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc`.

The cause can be categorized as one of the following:

- A job (started by either the NetBackup Java authentication service or user service) no longer exists and did not report its result status.
- The NetBackup Java service cannot monitor a job (started by either the NetBackup Java authentication service or user service). The reason it cannot monitor is probably due to a lack of system resources (insufficient memory).
- The maximum number of non-transient Activity Monitor jobs (>100) has already been started.

**Recommended Action:** Do the following, as appropriate:

- If the problem persists, restart the NetBackup Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:  
See "Setting debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart the NetBackup Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, you can retrieve the details from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 510

**Message:** File already exists: *file\_name*

**Explanation:** The NetBackup Java user service try to create a file that already exists.

**Recommended Action:** Remove the file, which can be identified in the user service log files.

See "Troubleshooting error messages in the NetBackup Administration Console" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 511

**Message:** NetBackup Java application server interface error.

**Explanation:** In some instances, this message concludes with

`Check the log file for more details.`

This generic error for all non-socket IO/connection-broken related errors (status code 507) can occur when data is processed from the NetBackup Java authentication or user services. The Java exception provides some additional detail about the error.

This error usually results from system or network problems.

**Recommended Action:** Do the following, as appropriate:

- If the problem persists, restart the NetBackup Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart the NetBackup Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, the details can be retrieved from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 512

**Message:** Internal error - a bad status packet was returned by NetBackup Java application server that did not contain an exit status code.

**Explanation:** The NetBackup Java authentication or user service returned a data packet that indicated an error, but no status code or error message was contained within it.

**Recommended Action:** Do the following, as appropriate:

- If the problem persists, restart the NetBackup Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart the NetBackup Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, the details can be retrieved from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 513

**Message:** bpjava-msvc: the client is not compatible with this server version (*server\_version*).

**Explanation:** The NetBackup Java application server (on the remote host you log in to) is not the same version as the NetBackup Java interface on your local host. The two are therefore incompatible.

**Recommended Action:** Do the following, as appropriate:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the computer that is specified in the logon dialog box or the local host where you started the NetBackup Java interface.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 514

**Message:** NetBackup Java: bpjava-msvc is not compatible with this application version (*application\_version*). You may try logon to a different NetBackup host or exit the application. The remote NetBackup host has to be configured with the same version of NetBackup as the host you started the application on.

**Explanation:** In some instances, this message concludes with

Check the log file for more details.

The NetBackup Java application server (on the remote host you log in to) is not the same version as the NetBackup Java interface on your local host. The two are therefore incompatible.

**Recommended Action:** Do the following, as appropriate:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the specified computer in the logon dialog box or the local host where you started the NetBackup Java interface.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 516

**Message:** Could not recognize or initialize the requested locale - (*locale\_NetBackup Java\_was\_started\_in*).

**Explanation:** This status concerns the UNIX locale configuration (or Windows regional settings) defined on the host that was specified in the NetBackup Java logon dialog box. At logon, the locale configuration is passed to the NetBackup Java authentication service. Status 516 is generated if the locale is not recognized or if the locale of the user service cannot be initialized.

The rules in the following files determine how a valid locale is recognized:  
`/usr/opensv/msg/.conf` on UNIX and `install_path\msg\lc.conf` on Windows.  
 When the locale is validated, initialization of the locale in the user service's environment is tried (by means of `setlocale`).

**Recommended Action:** On the specified host in the NetBackup Java logon dialog box, check the configuration file to ensure that a mapping is available for the indicated locale.

For information on locale configuration and mapping, refer to the [NetBackup Administrator's Guide, Volume II](#).

If there is a mapping, try to set the mapped locale on the host that was specified in the NetBackup Java logon dialog box. This system may not be configured properly.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 517

**Message:** Cannot connect to the NetBackup Java user service by VNETD on *host* on port *configured\_port\_number*. If successfully logged on beforehand, retry your last operation. Check the log file for more details.

**Explanation:** After the NetBackup Java authentication service validates the user name on the logon dialog box for access, all Administration console service requests use an NetBackup Java user service. Communication between the Administration console and user service is tried to host (host) on the specified port number in the error message by using VNETD. (The NetBackup Java configuration option NBJAVA\_CONNECT\_OPTION is set to 1.) The NetBackup Administration Console log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- On UNIX: Compare the VNETD entry in the `/etc/services` file with the VNETD\_PORT entry in `/usr/opensv/java/nbj.conf`  
On Windows: Compare the VNETD entry with the VNETD\_PORT entry in the `install_path\java\setconf.bat` file.  
These entries must match.
- Ensure that no other application uses the port that is configured for VNETD.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 518

**Message:** No ports available in range (*port\_number*) through (*port\_number*) per the NBJAVA\_CLIENT\_PORT\_WINDOW configuration option.

**Explanation:** All the ports in the specified range are in use. Too many users (concurrent) of the NetBackup Java interface or too few configured ports can cause this error.

**Recommended Action:** Do the following, as appropriate:

- Restart the NetBackup Java interface and try again.
- If the problem persists, increase the range of ports by changing the NBJAVA\_CLIENT\_PORT\_WINDOW option in the `/usr/opensv/java/nbj.conf` file (UNIX) or the `install_path\java\setconf.bat` file (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 519

**Message:** Invalid NBJAVA\_CLIENT\_PORT\_WINDOW configuration option value: (*option\_value*).

**Explanation:** The value for the NetBackup Java configuration option NBJAVA\_CLIENT\_PORT\_WINDOW is invalid.

**Recommended Action:** Correct the value in file `/usr/opensv/java/nbj.conf` (UNIX) or `install_path\java\setconf.bat` file (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 520

**Message:** Invalid value for NetBackup Java configuration option (*option\_name*): (*option\_value*).

**Explanation:** The specified NetBackup Java configuration option has an invalid value.

**Recommended Action:** Correct the value in file `/usr/opensv/java/nbj.conf` (UNIX) or `install_path\java\setconf.bat` file (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 521

**Message:** NetBackup Java Configuration file (*file\_name*) does not exist.

**Explanation:** The configuration file for the NetBackup Java interface was not found.

**Recommended Action:** Make sure that the configuration file the NetBackup Java interface exists and is properly formatted.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 522

**Message:** NetBackup Java Configuration file (*file\_name*) is not readable due to the following error: (*message*).

**Explanation:** The specified NetBackup Java configuration file exists but is not readable.

**Recommended Action:** Correct the file as specified in the message.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 523

**Message:** NetBackup Java application server protocol error.



**Explanation:** In some instances, this message concludes with the following:

Check the log file for more details.

The NetBackup Java interface received an incorrectly formatted protocol sequence from its application server.

**Recommended Action:** Do the following, as appropriate:

- If the problem persists, restart the NetBackup Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart the NetBackup Java interface and examine the logs.

---

**Note:** The error is probably the result of a system resource issue. When detailed debug logging ID is enabled, the details can be retrieved from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 525

**Message:** Cannot connect to the NetBackup Java authentication service by VNETD on (*host*) on port (*vnetd\_configured\_port\_number*). Check the log file for more details.

**Explanation:** The NetBackup Java authentication service authenticates the user name that is provided in the logon dialog box. Communication between the NetBackup Administration Console and the authentication service is tried to host *host* on the configured VNETD port number that error message specifies. The NetBackup Administration Console log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- On UNIX: Compare the VNETD entry in the `/etc/services` file with the VNETD\_PORT entry in `/usr/opensv/java/nbj.conf`  
On Windows: Compare the VNETD entry with the VNETD\_PORT entry in the `install_path\java\setconf.bat` file.  
These entries must match.
- Ensure that no other application uses the port that is configured for VNETD.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 526

**Message:** bpjava authentication service connection failed

**Explanation:** Cannot connect to the bpjava authentication service by NetBackup PBX at port 1556 (default).

**Recommended Action:** Do the following, as appropriate:

- If the target server is running an invalid version of NetBackup, the Java GUI attempts a further connection by the VNETD port 13724. No action is required.
- Check that the PBX service or daemon has been started on the server and that NetBackup services are running.
- Check if the Java GUI properties (`java/nbj.conf`) have been set up to connect to a PBX port other than 1556.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 527

**Message:** bpjava user service connection if connection to pbx on port 1556 fails

**Explanation:** Unable to connect to the bpjava user service using NetBackup PBX at port 1556 (default).

**Recommended Action:** Do the following, as appropriate:

- Check that the PBX service or daemon has been started on the server and that NetBackup services are running.
- If the target server is running an invalid version of NetBackup, the Java GUI attempts a further connection by the VNETD port 13724. No action is required.
- Check if the Java GUI properties (`java/nbj.conf`) have been modified to attempt a PBX port other than 1556.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 537

**Message:** Connection to the NetBackup database was not successful. Ensure that the database service is running.

**Explanation:** The NetBackup database service should be running while the Account Lockout option is enabled.

**Recommended Action:** Start the NetBackup database service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 538

**Message:** unable to login

**Explanation:** Verification of the X.509 certificate failed while connecting to the bpjava user on the host. This error can be caused by a clock skew between the NetBackup host and this computer. This issue occurs when the difference in time between the host from where you invoke the Remote Administration Console and the master server is greater than 24 hours.

**Recommended Action:** Synchronize the time on both hosts or decrease the difference in time to less than 24 hours.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 552

**Message:** The Certificate Revocation List (CRL) could not be downloaded and, therefore, the certificate revocation status could not be verified. For more information, see the NetBackup logs.

**Explanation:** The Certificate Revocation List (CRL) could not be downloaded. The possible causes include the following:

- The `certmapinfo.json` file is missing.
- The `certmapinfo.json` file does not contain the CRL path.
- The CRL file is missing.
- The CRL file is corrupted.
- The CRL file could not be locked.
- The CRL file could not be unlocked.

**Recommended Action:** For more information, see the `bpjava` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 600

**Message:** an exception condition occurred

**Explanation:** The synthetic backup job encountered an exception condition.

**Recommended Action:** Contact customer support and send the appropriate debug logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 601

**Message:** unable to open listen socket

**Explanation:** The `bpsynth` process cannot open a socket to listen for incoming connections from the `bptm` or the `bpdm` processes that were started for the following: for reading backup images or for writing the synthetic image on the media servers.

**Recommended Action:** Check the OS error that was reported in the error message, which `bpsynth` logged in the NetBackup error log. This error helps to diagnose the problem. Ensure that the `bpsynth` binary matches the installed NetBackup version. Retry the synthetic backup job. If the problem persists, contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 602

**Message:** cannot set non-blocking mode on the listen socket

**Explanation:** The `bpsynth` process is unable to set the non-blocking socket option on the listen socket.

**Recommended Action:** Check the OS error that was reported in the error message, which was logged in the NetBackup error log. The error helps to diagnose the problem. Ensure that the `bpsynth` binary matches the installed NetBackup version. If the condition persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 603

**Message:** cannot register handler for accepting new connections

**Explanation:** The `bpsynth` process cannot register the listen socket with the ACE reactor.

**Recommended Action:** Ensure that the `bpsynth` binary matches the installed NetBackup version. Retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 604

**Message:** no target storage unit specified for the new job

**Explanation:** A mismatch occurred between the storage units that are known to NetBackup and the specified target storage unit.

**Recommended Action:** Retry the synthetic backup job. If the problem persists, contact customer support and provide appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 605

**Message:** received error notification for the job

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 606

**Message:** no robot on which the media can be read

**Explanation:** `bpsynth` returns this error when it cannot find a robot on which to read a particular media ID that contains backup images to be synthesized. The media ID is included in the message that `bpsynth` logs. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 607

**Message:** no images were found to synthesize

**Explanation:** The database query to obtain the images to synthesize for the given policy did not return any images.

**Recommended Action:** Ensure that a synthetic full backup has one full image (real or synthetic) and one or more subsequent incremental images (differential or cumulative) to synthesize. For a cumulative synthetic backup, there must be two or more incremental (differential or cumulative) images to synthesize. Adjust your schedules so the appropriate backup jobs complete successfully before the synthetic job is run. The scheduler does not retry a synthetic backup job that fails with this error code.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 608

**Message:** storage unit query failed

**Explanation:** The database query to obtain all storage units failed.

**Recommended Action:** Verify that the `bpdgm` process is running and that no errors were logged to the NetBackup error log. Restart the `bpdgm` process (on UNIX), or the NetBackup Database Manager Service (on Windows) and retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 609

**Message:** reader failed

**Explanation:** The `bptm` or the `bpdgm` reader process was terminated with an error.

**Recommended Action:** See the NetBackup error log for the errors that the `bpsynth` and `bptm` or `bpdgm` reader logged. The error message should contain the actual error that the `bptm` or the `bpdgm` reader reports.

See the [NetBackup Troubleshooting Guide](#) for information on the error that the `bptm` or the `bpdgm` reader reports. The media may not be present or is defective or the drive that was used for reading the media is defective. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 610

**Message:** endpoint terminated with an error

**Explanation:** An error indication was received on the connection to the `bptm` or the `bpdgm` process.

**Recommended Action:** Review the errors in the NetBackup error log that the following processes logged: `bpsynth` and `bptm` or `bpdn`. Refer to the debug logs for these processes for more information. The connection may have broken due to the following: an error condition that the `bptm` or the `bpdn` process detects or network problems between the master and the media server. Check the network connectivity between the master and the media server. Retry the job and if the problem persists, contact customer support, and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 611

**Message:** no connection to reader

**Explanation:** A connection to the `bptm` or the `bpdn` reader process does not exist to communicate with the reader.

**Recommended Action:** This error should not occur. Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 612

**Message:** cannot send extents to `bpsynth`

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 613

**Message:** cannot connect to read media server

**Explanation:** The `bpsynth` process was unable to connect to the media server to read a backup image.

**Recommended Action:** Ensure that network connectivity exists between the master server and the specified media server. Examine the NetBackup error log for any error messages that `bpsynth` logged. For more information, refer to the debug logs for `bpsynth` on the master server and `bpcd` and `bptm` or `bpdm` on the media server.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 614

**Message:** cannot start reader on the media server

**Explanation:** The `bpsynth` process was unable to start the `bptm` or the `bpdm` process to read a backup image to be synthesized.

**Recommended Action:** Do the following, as appropriate:

- Examine the NetBackup error log for any errors that `bpsynth` logged. For more information, refer to the following debug logs: for `bpsynth` on the master server and for `bpcd` and `bptm` or `bpdm` on the media server. Ensure that the `bptm` or the `bpdm` binaries on the media server are executable and are not corrupt. Try running `bptm` or `bpdm` commands locally on the media server to ensure that the binary is executable and not corrupt. For instance, you can run the following command

```
/bp/bin/bptm -count -rn 0 -rt 8
```

where robot number is 0 and the robot type is 8. The robot type that corresponds to the robot number can be taken from the command line that is logged in the debug log for `bptm`. This command displays the counts for the up, shared, and assigned drives in the robot.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 615

**Message:** internal error 615

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs. A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 616

**Message:** internal error 616

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs. A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 617

**Message:** no drives available to start the reader process

**Explanation:** No drives are available to start the `bptm` process to read a backup image to be synthesized.

**Recommended Action:** Ensure that sufficient drives are available before you restart the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 618

**Message:** internal error 618

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 619

**Message:** internal error 619

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 620

**Message:** internal error 620

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 621

**Message:** unable to connect to `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 622

**Message:** connection to the peer process does not exist

**Explanation:** The underlying connection to the peer `bptm` or `bpdm` process does not exist. This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 623

**Message:** execution of a command in a forked process failed

**Explanation:** The failure normally occurs during the execution of a command on a media server through `bpcd`. Examine the NetBackup error log for additional error messages. Also refer to the debug logs for `bpsynth` (on the master server) and `bpcd` (on the media server) to get an explanation of the failure. A common cause of the failure is insufficient memory, file system full, or insufficient swap space.

**Recommended Action:** Retry the job and if the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 624

**Message:** unable to send a start command to a reader or a writer process on media server

**Explanation:** The `bpsynth` process is unable to send a command to the `bptm` or the `bpdm` process on the media server.

**Recommended Action:** Ensure that network connectivity exists between the master and the media server. Look for additional error messages in the NetBackup error log. More detailed information is present in the debug logs for `bpsynth` (on master server) and `bptm` or `bpdm` on the media server. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 625

**Message:** data marshalling error

**Explanation:** Problems were encountered while sending data over the connection. This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 626

**Message:** data un-marshalling error

**Explanation:** Problems were encountered in the parsing of the messages that `bpsynth` received. This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 627

**Message:** unexpected message received from bpsynth

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 628

**Message:** insufficient data received

**Explanation:** This error occurs in the following situation: partial data is read from the input socket and cannot be parsed until the remaining data that comprises the message is read. The lower layers encounter this error; it should not cause a process to be terminated.

**Recommended Action:** If this error causes the `bpsynth` binary to hang or malfunction, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 629

**Message:** no message was received from bptm

**Explanation:** This error is returned when no message is received from the `bptm` process in response to the command or query that was executed by using `bptm`.

**Recommended Action:** Look for additional error messages in the following logs: the NetBackup error log and the debug logs for `bpsynth` on the master server and `bptm` on the media server. A system condition (insufficient memory, file system full, insufficient swap space) on the media server may prevent the `bptm` process from sending the response. Verify the network connectivity between the master and the media server. If no explanation is found for the failure and the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 630

**Message:** unexpected message was received from `bptm`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 631

**Message:** received an error from `bptm` request to suspend media

**Explanation:** The `bpsynth` process was unable to suspend a media that contained one or more images to be synthesized. A message in the `bpsynth` legacy log lists the media IDs to be suspended. The `bpsynth` log also includes a failure message to indicate which particular media in the list was not suspended. `media (ordinal)` indicates the unsuspended media by means of its order in the list. For example, if the unsuspended media was the second media in the list, the failure message says `media (1)`.

**Recommended Action:** Examine the `bptm` debug log for more information on the reason for the suspend failure. The `bpsynth` process ignores this error and continues to process. It has the potential to fail later if the media with the images to be read gets assigned to another backup or restore job. If the synthetic backup job fails, fix the condition that lead to the suspend failure and retry the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 632

**Message:** received an error from `bptm` request to un-suspend media

**Explanation:** The `bpsynth` process was unable to un-suspend a media that it suspended at the start of the synthetic backup job. A message in the `bpsynth` legacy log lists the media IDs to be un-suspended. The `bpsynth` log also includes a failure message to indicate which particular media in the list was not un-suspended. `media (ordinal)` indicates the media by means of its order in the list. For example, if the media that was not un-suspended was the second media in the list, the failure message says `media (1)`.

**Recommended Action:** Look at the debug log for the `bptm` process on the media server for an explanation of the un-suspend failure and the media ID. Try to un-suspend the tape manually by using the `bpmmedia` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 633

**Message:** unable to listen and register service by vneta

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 634

**Message:** no drives available to start the writer process

**Explanation:** The `bpsynth` process cannot start the synthetic backup job because no drives were available in the target storage unit for the writer. The storage unit may be in use by a restore or another synthetic backup job.

**Recommended Action:** Ensure that the target storage unit that is configured for the synthetic backup schedule has an available drive to write the synthetic backup image.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 635

**Message:** unable to register handle with the reactor

**Explanation:** Unable to register a handle with the ACE reactor to monitor events on the handle. This error can occur in `bpsynth`.

**Recommended Action:** Examine NetBackup error log for any errors that were logged for the job. Refer to the debug logs for `bpsynth` for more information. Retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 636

**Message:** read from input socket failed

**Explanation:** The read from an input socket failed. The underlying connection has been broken.

**Recommended Action:** The `bpsynth` process encountered an error while reading from an input socket. The socket may be between `bpsynth` and `bptm` or `bpdm`.

The `errno` that was logged to the NetBackup error log indicates the reason for the failure. For more information, refer to the following: the debug log for `bpsynth` (on the master server) and for the `bptm` or the `bpdm` reader or writer processes (on the media server). Check the network connectivity between the master and the media server. Rerun the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 637

**Message:** write on output socket failed

**Explanation:** The write to an output socket failed. The underlying connection has been broken.

**Recommended Action:** The `bpsynth` process encountered an error while writing to an output socket. The socket is between `bpsynth` and `bptm` or `bpdm`.

The `errno` that logged to the NetBackup error log indicates the reason for the failure. For more information, refer to the following: the debug log for `bpsynth` (on the master server) and for the `bptm` or the `bpdm` reader or writer process (on the media server). Check the connectivity between the master and the media server. Retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 638

**Message:** invalid arguments specified

**Explanation:** The `bpsynth` command fails with this error code if incorrect arguments were specified.

**Recommended Action:** Refer to the `bpsynth` command line arguments (by using `-help`) for the correct argument specification. If the synthetic backup job was started manually by the command line, correct the arguments to `bpsynth` and rerun the job. If the synthetic backup job was scheduled or started with the console, ensure that the `bpsynth` and the `nbjm` binaries match the installed NetBackup version.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 639

**Message:** specified policy does not exist

**Explanation:** The policy that was specified on the `bpsynth` command does not exist in the database. Either the command line or `nbjm` initiated the `bpsynth` command. If `nbjm` initiated it, the policy may have been deleted after `nbjm` started `bpsynth` and before `bpsynth` issued the database query.

**Recommended Action:** If `bpsynth` is initiated with the command line, rerun the command for an existing policy. If the problem persists after you verify the following, contact customer support and send the appropriate logs:

- The synthetic backup job was scheduled or started by using the **NetBackup Administration Console** (manual start).
- The policy exists in the `bpllist` command configuration.
- Check the logs for `nbjm`, which uses unified logging (OID 117).

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 640

**Message:** specified schedule was not found

**Explanation:** The schedule on the `bpsynth` command did not exist in the specified policy definition in the database due to either of the following:

- The command line initiated the `bpsynth` command
- The specified schedule was deleted from the policy after `nbjm` started `bpsynth`, before `bpsynth` issued the database query.

**Recommended Action:** If the command line initiated `bpsynth`, do the following: rerun the command with the correct synthetic schedule label defined in the policy of the synthetic backup job to be run. If the synthetic backup job was scheduled or started with the **NetBackup Administration Console**, define a new schedule in the policy and retry the job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 641

**Message:** invalid media type specified in the storage unit

**Explanation:** The media type that was specified in the target storage unit is invalid for synthetic backup. Synthetic backup images can only be written to disk, disk staging, and Media Manager type of storage units.

**Recommended Action:** Ensure that the target storage unit that was configured for synthetic backup is a disk, disk staging, or Media Manager type (not NDMP type). Rerun synthetic backup with the appropriate storage unit.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 642

**Message:** duplicate backup images were found

**Explanation:** The database query returned duplicate backup IDs. This error should not occur.

**Recommended Action:** Contact customer support and send the appropriate logs. A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 643

**Message:** unexpected message received from `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs. A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 644

**Message:** extent directive contained an unknown media ID

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 645

**Message:** unable to start the writer on the media server

**Explanation:** The `bpsynth` process was unable to start the following: the `bptm` or the `bpdm` process on the media server that is associated with the target storage unit to write the synthetic image.

**Recommended Action:**

Examine the NetBackup error log for any messages that `bpsynth` logged. For more information, refer to the following: the debug logs for `bpsynth` on the master server and `bpcd` and `bptm` or `bpdm` on the media server. Ensure that the `bptm` or the `bpdm` binaries on the media server are executable and are not corrupt. Try to run the `bptm` or the `bpdm` commands locally on the media server to ensure that the binary is executable and not corrupt. For instance, you can run the following command:

```
install_path/netbackup/bin/bptm -count -rn 0 -rt 8
```

where robot number is 0 and robot type is 8. The robot type that corresponds to the robot number can be taken from the command line that is logged in the debug log for `bptm`. This command displays the counts for the up, shared, and assigned drives in the robot. In case the synthetic image is to be written to a disk storage unit, verify the `bpdm` binary by running the following command:

```
install_path/netbackup/bin/bpdm
```

It should print the following:

```
bpdm: media manager operation not specified
```

Retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 646

**Message:** unable to get the address of the local listen socket

**Explanation:** The `bpsynth` process cannot obtain the address of the opened listen socket. The `bpsynth` process needs the address to receive incoming connections from the `bptm` or the `bpdm` processes, which were started to read the source images. This problem should not happen. The library call used to retrieve the address of the listen socket relies on the underlying system call to obtain the socket address. The `errno` that the system call reports is included in the error message and should help to diagnose the problem.

**Recommended Action:** Rerun the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 647

**Message:** validation of synthetic image failed

**Explanation:** This error is returned when `bpsynth` receives an error from the database call to validate the synthetic image.

**Recommended Action:** This error may indicate a problem in the synthetic backup process. Examine the NetBackup error log for any messages that the following processes logged: `bpsynth` and `bptm` or `bpdm`. Look at the debug logs for these processes for additional information. If you cannot resolve the problem, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 648

**Message:** unable to send extent message to BPXM

**Explanation:** The `bpsynth` process cannot send extent information to the `bptm` or the `bpdm` process that was started to read a specified backup image to synthesize.

**Recommended Action:** This error indicates a communication problem between `bpsynth` and the `bptm` or the `bpdm` reader process on the media server. Ensure that the media server is accessible and that the `bptm` or the `bpdm` process is running on the media server. Examine the NetBackup error log for any errors that the following logged: `bpsynth` (on the master server) and the `bptm` or the `bpdm` reader process (on the media server). Examine the debug logs for `bpsynth` and `bptm` or `bpdm` for additional information. Rerun the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 649

**Message:** unexpected message received from BPXM

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 650

**Message:** unable to send extent message to `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 651

**Message:** unable to issue the database query for policy

**Explanation:** The `bpsynth` process was unable to send the database query for policy.

**Recommended Action:** This error indicates a communication problem between `bpsynth` and `bpdbm`. Ensure that `bpdbm` is running and the `bpdbm` binary matches the installed NetBackup version. Examine the NetBackup error log for any errors that `bpdbm` and `bpsynth` logged. Examine the debug logs for `bpsynth` and `bpdbm` for additional information. Restart the `bpdbm` process (on UNIX) or the NetBackup Database Manager Service (on Windows) and rerun the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 652

**Message:** unable to issue the database query for policy information

**Explanation:** The `bpsynth` process was unable to send the database query for detailed information about the policy.

**Recommended Action:** This error indicates a communication problem between `bpsynth` and `bpdbm`. Ensure that `bpdbm` is running. Examine the NetBackup error log for any errors that `bpdbm` and `bpsynth` logged. Examine the debug logs for `bpsynth` and `bpdbm` for additional information. Restart the `bpdbm` process (on UNIX) or the NetBackup Database Manager Service (on Windows) and rerun the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 653

**Message:** unable to send a message to `bpccord`



**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 654

**Message:** internal error 654

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 655

**Message:** no target storage unit was specified by command line

**Explanation:** No target storage unit was specified on the `bpsynth` command line (-S).

**Recommended Action:** Rerun `bpsynth` with the target storage unit specified by the -S option.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 656

**Message:** unable to send start synth message to `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 657

**Message:** unable to accept connection from the reader

**Explanation:** The `bpsynth` process was unable to accept the connection from the `bptm` or the `bpdm` reader process that runs on the media server.

**Recommended Action:** Examine the NetBackup error log for any errors that `bpsynth` and `bptm` or the `bpdm` reader process logged. The message that `bpsynth` logged includes the error (`errno`) reported by the system call. Refer to the debug logs for `bpsynth` on the master server and `bptm` or the `bpdm` process on the media servers for more information. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 658

**Message:** unable to accept connection from the writer

**Explanation:** The `bpsynth` process was unable to accept the connection from the `bptm` or the `bpdm` writer process that runs on the media server.

**Recommended Action:** Examine the NetBackup error log for any errors that `bpsynth` and the `bptm` or the `bpdm` writer process logged. The message that `bpsynth` logged includes the error (`errno`) reported by the system call. Also refer to the debug logs for `bpsynth` on the master server and `bptm` or the `bpdm` process on the media server for more information. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 659

**Message:** unable to send a message to the writer child process

**Explanation:** The `bpsynth` process was unable to send the message that contains the following to the `bptm` or the `bpdm` writer: the host name and the port number of the `bptm` or the `bpdm` reader.

**Recommended Action:** Examine the NetBackup error log for any errors that `bpsynth` and the `bptm` or the `bpdm` writer process logged. Refer to the following for more information: the debug logs for `bpsynth` on the master server and the `bptm` or the `bpdm` process on the media server. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 660

**Message:** a synthetic backup request for media resources failed

**Explanation:** The request for resources failed due to an internal NetBackup error.

**Recommended Action:** Create logs as explained in the following topic:

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Rerun the job and send the logs to customer support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 661

**Message:** unable to send exit message to the BPXM reader

**Explanation:** The `bpsynth` process cannot send the exit message to indicate the end of extents messages to the following: `bptm` or the `bpdm` reader process on the

media server. The network connection between the master and the media server may have terminated or the `bptm` or the `bpdm` reader process has terminated.

**Recommended Action:** Check the network connectivity between the master and the media server. Examine the NetBackup error log for any errors that `bpsynth` and `bptm` or the `bpdm` reader process logged. Examine the debug logs for `bpsynth` on the master server and `bptm` or the `bpdm` reader process on the media servers for more detailed information. If the problem persists, contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 662

**Message:** unknown image referenced in the synth context message from BPXM

**Explanation:** The `bpsynth` process received an extent message from the `bptm` or the `bpdm` reader with reference to a media ID that was unknown to `bpsynth`. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 663

**Message:** image does not have a fragment map

**Explanation:** The `bpsynth` process received an image without a fragment map from `bpdbm`. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 664

**Message:** zero extents in the synthetic image, cannot proceed

**Explanation:** The `bpsynth` process receives zero extents from `bpdbm`. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 665

**Message:** termination requested by `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 667

**Message:** unable to open pipe between `bpsynth` and `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 668

**Message:** pipe fgets call from bpcoord failed

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 669

**Message:** bpcoord startup validation failure

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 670

**Message:** send buffer is full

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See "Logs to accompany problem reports for synthetic backups" in the [NetBackup Logging Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 671

**Message:** query for list of component images failed

**Explanation:** A new synthetic image cannot be formed because of a problem with the required component images. For example: a new, synthetic full backup is tried from the previous full image from Sunday and from the five differential incremental images from Monday through Friday. This error occurs if any of those images (except the most recent image on Friday) have expired.

**Recommended Action:** Run a non-synthetic backup (either a new full or new cumulative), depending on the type of backup that failed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 800

**Message:** resource request failed

**Explanation:** The `nbgm` process was unable to get the required resources for a job. An EMM reason string that appears in the Activity Monitor job details display and in the `nbgm` debug log accompanies this status code. The EMM reason string identifies the reason for the failed resource request.

**Recommended Action:** Locate the EMM reason string, correct the problem, and rerun the job.

Some generic EMM reason strings (such as `Disk volume is down`) may require generating some reports to determine the cause of the failure. Generate the report by using either `bpererror` or various log entry reports, such as **Reports > Disk Reports > Disk Logs** in the **NetBackup Administration Console**.

Click [here](#) to view technical notes and other information in the Veritas knowledge base about this status code.

## NetBackup status code: 801

**Message:** JM internal error

**Explanation:** The `nbgm` process encountered an internal error.

**Recommended Action:** If the problem persists, submit a report with the following items.

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbgm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).

- Legacy logs:
  - On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompatd`, `bpdbrm`, and `nbproxy`
  - On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdm`
  - On the client for `bpcd` and `bpbkarr`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdbrjobs` output: run `bpdbrjobs` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 802

**Message:** JM internal protocol error

**Explanation:** `nbjm` returns this error whenever a protocol error occurs with an external process that tries to communicate with `nbjm`. External processes include `bptm`, `tpreq`, `bplabel`, `dqts`, `vmphyinv`, or `nbpem`.

**Recommended Action:** Ensure that the NetBackup software on the master and the media server is from an official NetBackup release.

If the problem persists, submit a report with the following items.

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbjm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- Legacy logs:
  - On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompatd`, `bpdbrm`, and `nbproxy`
  - On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdm`
  - On the client for `bpcd` and `bpbkarr`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.



- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdjobs` output: run `bpdjobs` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 803

**Message:** JM terminating

**Explanation:** A service request for an existing or a new job was received when the `nbjm` process shutdown.

**Recommended Action:** If `nbjm` was not terminated explicitly (by entering the `/usr/opensv/netbackup/bin/bp.kill_all` command on UNIX or `install_path\NetBackup\bin\bpdown` on Windows), submit a report with the following items.

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbjm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- Legacy logs:
  - On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompad`, `bpbm`, and `nbproxy`
  - On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdm`
  - On the client for `bpcd` and `bpbkar`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdjobs` output: run `bpdjobs` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 805

**Message:** Invalid jobid

**Explanation:** The `nbjm` process received an invalid job ID in the request.

### Recommended Action:

The requested operation may refer to a job that no longer exists or is not known to nbjm. Or the job ID is invalid (less than or equal to 0). Ensure that the command used to start the job did not specify a job ID already in use by another job.

If the problem persists, submit a report with the following items.

- Unified logging files on the NetBackup server for nbpem (originator ID 116), nbjm (117), nbrb (118), and PBX (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- Legacy logs:
  - On the NetBackup master server for bpbrm, bpjobd, bpcompatd, bpbm, and nbproxy
  - On the media server for bpcd, bpbrm, and bptm or bpdm
  - On the client for bpcd and bpbkar

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, you must create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- bpdjobs output: run bpdjobs to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 806

**Message:** this mpx group is unjoinable

**Explanation:** This error is a timing problem. It can happen if the job was added to a multiplexed group when bpbrm terminates due to an error condition. The Resource Broker (nbrb) does the allocation of a multiplexed group and the Job Manager (nbjm) starts and monitors the bpbrm process.

**Recommended Action:** If the failed job is scheduled and the retry count allows it, nbpem submits the job again. If the failed job was initiated manually, submit it again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 807

**Message:** not externalized

**Explanation:** Not available.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 811

**Message:** failed to communicate with resource requester

**Explanation:** Job Manager (`nbgm`) tries to notify a process (usually `bptm`) of the status of a resource it requested. That notification fails because of a communication problem.

**Recommended Action:** Do the following, as appropriate:

- Verify the connectivity between the master and the media server.
- Verify the Private Branch Exchange (PBX) configuration and permissions. More information on PBX is available.  
See "Resolving PBX problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 812

**Message:** failed to communicate with Resource Broker

**Explanation:** The Job Manager (`nbgm`) tries to make a request to the Resource Broker (`nbrb`). The request fails because of a communication problem.

**Recommended Action:** Do the following, as appropriate:

- Verify the connectivity between the master server and the EMM server.
- Verify the Private Branch Exchange (PBX) configuration and permissions. More information on PBX is available.  
See "Resolving PBX problems" in the [NetBackup Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 813

**Message:** duplicate reference string specified

**Explanation:** The reference string is the file name specified on the `-f` option of the `tpreq` command. The specified file name on `tpreq` is already in use by another `tpreq`.

**Recommended Action:** Choose a unique name that is not already in use.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 818

**Message:** retention level mismatch

**Explanation:** A job fails with this error code if the retention level of the allocated media does not match the retention level that is configured in the policy.

**Recommended Action:** Contact NetBackup Technical Support and provide relevant supporting materials.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 819

**Message:** unable to communicate with JM proxy

**Explanation:** The Job Manager cannot communicate with nbproxy.

**Recommended Action:** Restart the Job Manager. If the condition persists, please contact NetBackup Support and provide relevant supporting materials.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 823

**Message:** no BRMComm to join

**Explanation:** The job was unable to join the multiplex group. This error is an internal error.

**Recommended Action:** Submit a report with the following items.

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbjm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- The following legacy logs:

- On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompad`, `bpdbrm`, and `nbproxy`

- On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdbrm`

- On the client for `bpcd` and `bpbkarr`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdbrm` output: run `bpdbrm` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 830

**Message:** drive(s) unavailable or down

**Explanation:** All configured drive that can be used for this job are down.

One of the following has occurred:

- No drives are configured for the media that was requested for the job.
- The job requires an NDMP drive path, but no NDMP drive paths are up or configured.
- The job cannot use an NDMP drive path, but these are the only drive paths that are up or configured for the drive.

**Recommended Action:** Do the following:

- Make sure that the drives and drive paths are up and correct for the media that you configure.
- Verify that `ltid` is running on the required media server, and that the media server is active for tape.
- Use the device monitor to startup the drives paths if they are down.
- If the drives are downed again, clean the drives.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 831

**Message:** image has been validated

**Explanation:** A job retry attempt fails because the image from the previous attempt has already been validated. This error can occur if `nbjm` shuts down before it receives the job success status. This status code indicates a timing problem only.

**Recommended Action:** No corrective action is required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 832

**Message:** failed to write discover data to a file

**Explanation:** The Job Manager (`nbjm`) is unable to write a temporary file in the `netbackup/bin/bpsched.d` directory.

**Recommended Action:** Make sure that the file system is not full.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 833

**Message:** error parsing discovered XML data

**Explanation:** The Job Manager was unable to parse the XML document that was returned from discovery. This error is an internal error.

**Recommended Action:** Submit a report with the following items:

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbjm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- The following legacy logs:
  - On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompatd`, `bpdgm`, and `nbproxy`
  - On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdm`
  - On the client for `bpcd` and `bpbkarr`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX) or `install_path\Netbackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdjobs` output: run `bpdjobs` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 900

**Message:** retry nbrb request later

**Explanation:** The NetBackup Resource Broker (`nbrb` service) was unable to respond to a request.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- If necessary, set global logging to a higher level by using **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 901

**Message:** RB internal error

**Explanation:** The NetBackup Resource Broker (`nbrb` service) encountered an internal error.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- If necessary, set global logging to a higher level, by using **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 902

**Message:** RB invalid argument

**Explanation:** The NetBackup Resource Broker (`nbrb` service) detected an invalid argument.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- If necessary, set global logging to a higher level, by using **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 903

**Message:** RB communication error

**Explanation:** The NetBackup Resource Broker (`nbrb` service) encountered a communication error.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- If necessary, set global logging to a higher level, by using **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 904

**Message:** RB max reallocation tries exceeded

**Explanation:** Under some conditions, failed mounts are retried; the number of retries for the resource request has been exceeded.

**Recommended Action:** For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118) and for `nbemm` (originator ID 111). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows). Also examine the legacy `bptm` log.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 905

**Message:** RB media server mismatch

**Explanation:** If you have any storage units that are specified for multiple copies, they must be on the same media server.

**Recommended Action:** Do the following, as appropriate:

- Configure the backup schedule with a storage unit or storage unit groups that can be run on the same media server.
- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 906

**Message:** RB operator denied mount request

**Explanation:** By using the **Device Management** node in the **NetBackup Administration Console** or the `vmopr cmd` command, the operator denied a mount request.

**Recommended Action:** Do the following, as appropriate:

- Determine the cause of the mount request denial and retry the job.
- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 907

**Message:** RB user canceled resource request

**Explanation:** A user-initiated action caused a Resource Broker (`nbrb`) request to be canceled.

**Recommended Action:** Do the following, as appropriate:

- Determine the action that resulted in cancelation of the resource request.

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 908

**Message:** RB was reset

**Explanation:** The NetBackup Resource Broker (`nbrb`) resources and database were reset. Any `nbrb` requests that remain may fail when RB is reset. (An example of a process that resets the database is catalog recovery.)

**Recommended Action:** Do the following, as appropriate:

- Determine the action that reset `nbrb` resources and the `nbemm` database.
- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). All unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 912

**Message:** RB disk volume mount failed

**Explanation:** The attempt to mount a disk volume failed. Possible reasons are hardware problems, inconsistent EMM database, or a NetBackup Resource Broker (`nbrb`) error.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the `nbrb` service (originator ID 118). Unified logging is written to `/usr/opensv/logs` (UNIX) or `install_path\NetBackup\logs` (Windows).
- If necessary, set global logging to a higher level: **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 914

**Message:** RB media reservation not found

**Explanation:** The read media for a duplicate or synthetic backup job must be reserved at the start of the job. Status 914 occurs when the NetBackup Resource Broker (*nbrb*) receives an allocation request for a read media that was never reserved. It can result from an internal error in *bpduplicate*, *nbrb*, or *nbrb*.

**Recommended Action:** Do the following, as appropriate:

- Examine the unified logging files on the NetBackup server for the *nbrb* service (originator ID 118). Unified logging is written to */usr/openv/logs* (UNIX) or to *install\_path\NetBackup\logs* (Windows).
- If necessary, set global logging to a higher level: **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the *nbrb* logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 915

**Message:** RB disk volume mount must retry

**Explanation:** A shared disk job has failed because RB is unable to mount the disk volume. Shared disk requires that volume file systems be unmounted and remounted before other media servers can use them.

**Recommended Action:** Do the following, as appropriate:

- Verify that processes are not in the disk volume mount directories, which prevents them from being unmounted. If the problem persists, restart NetBackup on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 916

**Message:** Resource request timed out

**Explanation:** A job request for resources has failed because resources were not available before the configured time limit expired. Some jobs may specify a timeout when they ask for drives or other resources. If jobs consistently cause this error, more jobs may be scheduled than the number of available drives. The drives in the Resource Broker job queue are not completed soon enough to allow new jobs to start before they timeout.

**Recommended Action:** Distribute the scheduled job start times over a wider period of time.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 917

**Message:** RB multiplexing group not found

**Explanation:** The NetBackup Resource Broker (`nbrb`) has received a request for an unknown multiplex group ID. This error can be caused by a timing problem when RB is killed and restarted. It can also be caused by an internal error in `nbgm` or `nbrb`.

**Recommended Action:** Restart `nbgm` and `nbrb`. If the problem persists, write a problem report with the appropriate logs including the `nbgm` and `nbrb` logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 918

**Message:** RB does not have a multiplexing group that uses this media ID or drive name

**Explanation:** The NetBackup Resource Broker (`nbrb`) has received a request for an unallocated media or drive.

**Recommended Action:** The `nbrbutl` command may cause this error. Rerun the command with an allocated media ID or drive. Also, this error may be internal. If the problem persists, write a problem report with the appropriate logs including `nbgm` and `nbrb`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1000

**Message:** Client is offline

**Explanation:** An attempt was made to run a manual job for a client that is offline.

**Recommended Action:** Wait until the client is brought online or manually bring the client online by using the GUI or the `bpclient` command before you submit the manual job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1001

**Message:** discovery document error

**Explanation:** The Policy Execution Manager (`pem`) is unable to parse the XML document that was returned from the discovery operation. This error is an internal error.

**Recommended Action:** Submit a report with the following items.

- Unified logging files on the NetBackup server for `nbpem` (originator ID 116), `nbjm` (117), `nbrb` (118), and `PBX` (103). All unified logging is written to `/usr/opensv/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows).
- The following legacy logs:
  - On the NetBackup master server for `bpbrm`, `bpjobd`, `bpcompad`, `bpdbrm`, and `nbproxy`
  - On the media server for `bpcd`, `bpbrm`, and `bptm` or `bpdbrm`
  - On the client for `bpcd` and `bpbkar`

Legacy logs are in subdirectories under `/usr/opensv/netbackup/logs/` (UNIX and Linux) or `install_path\NetBackup\logs\` (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of `/usr/opensv/db/jobs/trylogs` (UNIX and Linux) or `install_path\NetBackup\db\jobs\trylogs` (Windows).
- `bpdbrm` output: run `bpdbrm` to obtain the state and status of all jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1002

**Message:** Discovery detected a failed client

**Explanation:** The query rules cannot exclude one or more clients, and these clients cannot be selected for backup. A host name problem may be the cause of this error.

**Recommended Action:** See the job details log for more specific information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1057

**Message:** A data corruption has been detected.

**Explanation:** The data consistency check detected a data loss or data corruption in the Media Server Deduplication Pool (MSDP) and reported the affected backups.

**Recommended Action:** Search `storaged.log` on the server for the affected backups and contact technical support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1058

**Message:** A data inconsistency has been detected and corrected automatically.

**Explanation:** The data consistency check detected a potential data loss and fixed it automatically in the Media Server Deduplication Pool (MSDP).

**Recommended Action:** Search the `storaged.log` file on the pertinent media server. Contact support to investigate the root cause if the problem persists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1401

**Message:** Invalid arguments received

**Explanation:** Invalid input arguments pass to the Hold Service.

**Recommended Action:** Ensure that all the required parameters are passed with the correct values.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1402

**Message:** Hold ID or Hold name argument is invalid

**Explanation:** The `nbholdutil` command contains an invalid `-holdid` or `-holdname` option that passes to the root Hold Service.

**Recommended Action:** Check the `-holdid` and `-holdname` options for valid values.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1403

**Message:** Backup ID argument is invalid

**Explanation:** The `nbholdutil` command contains an invalid `-backupid` option that passes to the root Hold Service.

**Recommended Action:** Check the `-backupid` option for a valid value.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1405

**Message:** No images are found.

**Explanation:** The `nbholdutil` command contains a `-backupid` for an image that cannot be found.

**Recommended Action:** Check that the `-backupid` option is for a valid image.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1407

**Message:** Invalid hold state

**Explanation:** This code is reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1408

**Message:** Database error

**Explanation:** The hold service fails to get hold related information.

**Recommended Action:** Make sure that the Hold database and the DBM services are running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1409

**Message:** Unable to connect to database

**Explanation:** The hold service fails to connect to the Hold database.

**Recommended Action:** Make sure that the Hold database and the DBM services are running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1410

**Message:** No data found

**Explanation:** No images or hold copies are found for the given values.

**Recommended Action:** Make sure that all the required parameters are passed with their correct values.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1411

**Message:** Catalog error

**Explanation:** You try to update the image catalog.

**Recommended Action:** Check that the image copy on which the hold operation is applied is valid and not expired.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1412

**Message:** Hold record is being updated

**Explanation:** A hold operation is in the process of being updated.

**Recommended Action:** Retry the operation at a later time or restart the `nbim` service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1413

**Message:** Requested hold is not found

**Explanation:** The `nbholdutil` command requests a hold that does not exist.



**Recommended Action:** Check the `-holdname` and `-holdid` options. You can use `nbholdutil -list` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1414

**Message:** Duplicate hold found

**Explanation:** You try to create a hold whose name is used by another hold.

**Recommended Action:** Try a different name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1415

**Message:** Duplicate image found

**Explanation:** Reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1416

**Message:** Partially failed due to duplicate image

**Explanation:** Reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1417

**Message:** Partially failed due to unhold image

**Explanation:** Backup image copy is already removed from the specified hold.

**Recommended Action:** Make sure that you provide the correct backup ID and that it is present in the current hold.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1418

**Message:** Requested image is not found

**Explanation:** The backup image with the specified backup ID is not found. Either the image is expired or the given backup ID is invalid.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1419

**Message:** Partially failed due to invalid image copy

**Explanation:** Reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1420

**Message:** Cannot expire on hold image copy.

**Explanation:** You try to expire an image copy (by using bpexpdate or the **NetBackup Administration Console**) that is on hold.

**Recommended Action:** Remove all holds from this backup image. Or remove holds from all images on this backup ID to expire the backup image.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1421

**Message:** Active holds cannot be changed

**Explanation:** You try to update a hold that is in an active state.

**Recommended Action:** Restart the NBIM service

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1422

**Message:** Cannot deassign media on hold

**Explanation:** The user tries to de-assign a media having an image copy that is on hold.

**Recommended Action:** Lift the holds on the image copies that are backed up on the media being de-assigned.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1423

**Message:** Unable to retrieve hold status of the image copies

**Explanation:** Reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1425

**Message:** Requested hold is not found

**Explanation:** The hold service cannot find holds with the specified hold name or hold ID.

**Recommended Action:** Use the `nbholdutil -list` to list all holds. Check that the specified `-holdname` and `-holdid` options are valid.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1426

**Message:** Retired holds cannot be changed

**Explanation:** Reserved for future use.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1500

**Message:** Storage unit does not exist or cannot be used where specified

**Explanation:** The storage unit or storage unit group that you specify for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified storage unit or storage unit group exists in the NetBackup database.
- Verify that the specified storage unit is not of type **BasicDisk** or **Staging**, because storage lifecycle policies do not support them.
- Verify that the storage unit is not specified for snapshot destinations in storage lifecycle policy. Snapshot destinations do not require a storage unit in the storage lifecycle policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1501

**Message:** Source operation cannot be used where specified

**Explanation:** The source that you specify for one or more duplication destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified source refers to a valid destination in the list of destinations in storage lifecycle policy.
- Verify that the **Backup** or **Snapshot** destination type does not have any source specified. If you use `nbstl` to configure storage lifecycle policy, use value zero (0) as the source for a backup or snapshot destination type.
- Verify that the destination that refers to the specified source is not a **Snapshot** destination type. NetBackup cannot duplicate a backup image that uses snapshot copy as a source.
- Verify that the specified source does not refer to the destination itself for which the source is mentioned.
- Verify that the specified list of destinations in a storage lifecycle has a circular dependency for the source.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1502

**Message:** Retention type cannot be used where specified

**Explanation:** The retention type that you specify for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the retention type that you specify in the storage lifecycle policy is either of **Fixed**, **Staged capacity managed**, or **Expire after duplication**.
- Verify that the **Expire after duplication** retention type is used for a destination only if it is specified as a source to other destinations in storage lifecycle policy.
- Verify that the **Staged capacity managed** retention type is used in storage lifecycle policy only for the disk destinations that support **Capacity management** capabilities.
- Verify that the **Snapshot** destination type in storage lifecycle policy uses **Fixed** retention type only.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1503

**Message:** Volume pool does not exist or cannot be used where specified

**Explanation:** The volume pool that you specify for one or more destinations in the storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified volume pool exists in NetBackup database.
- Verify that the volume pool is not specified for the **Backup** destination type in storage lifecycle policy.
- Verify that the volume pool is not specified for the **Snapshot** destination type in storage lifecycle policy.
- Verify that the volume pool is not specified for the **Duplication** destination type that uses disk storage units in storage lifecycle policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1504

**Message:** Server group does not exist or cannot be used where specified

**Explanation:** The media server group that you specify for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified media server group exists in NetBackup database.

- Verify that the media server group is not specified for **Backup** destination types in storage lifecycle policy.
- Verify that the server group is not specified for **Snapshot** destination types in storage lifecycle policy.
- Verify that the media server group is not specified for **Duplication** destination types that use disk storage unit in storage lifecycle policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1505

**Message:** alternate read server does not exist or cannot be used where specified

**Explanation:** The alternate read server that you specify for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified alternate read server exists in the NetBackup database.
- Verify that the alternate read server is not specified for **Backup** destination types in storage lifecycle policy.
- Verify that the alternate read server is not specified for **Snapshot** destination types in storage lifecycle policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1506

**Message:** data classification does not exist

**Explanation:** The data classification that you specify in the storage lifecycle policy is not valid.

**Recommended Action:** Verify that the specified data classification exists in the NetBackup database.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1507

**Message:** Invalid deferred operation flag

**Explanation:** The deferred operation flag is not valid for the SLP operation.

**Recommended Action:** Do the following:

- If you used the `nbstl -defop` command, make sure that the specified argument is one of the following: f, F, t, or T.  
For more information on the `nbstl` command, see the [NetBackup Commands Reference Guide](#).
- Make sure that the flag is not set for the primary SLP operations: Backup, snapshot, and import.
- Make sure that the source copy has fixed retention.
- Refer to the detailed log messages for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1508

**Message:** Storage lifecycle policy exceeds maximum copies

**Explanation:** The list of destinations that you specify in the storage lifecycle policy exceeds 10, the maximum number of allowed backup copies.

**Recommended Action:** Verify that the number of destinations that you specify in the storage lifecycle policy does not exceed 10.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1509

**Message:** Storage lifecycle policy exceeds maximum backup operations

**Explanation:** The number of **Backup** type destinations that you specify in storage lifecycle policy exceeds the maximum number of simultaneous copies allowed.

**Recommended Action:** Verify that the number of **Backup** type destinations that you specify in the storage lifecycle policy is less than or equal to 4. (The default value of the **maximum number of allowed simultaneous copies** parameter is 4.)

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1510

**Message:** storage lifecycle policy cannot have more than one snapshot operation

**Explanation:** The list of destinations that you specify in the storage lifecycle policy exceeds the maximum number of allowed snapshot destinations.

**Recommended Action:** Verify that the storage lifecycle policy is not configured with more than one “Snapshot” type of destinations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1511

**Message:** storage lifecycle policy must have at least one fixed retention or snapshot rotation operation

**Explanation:** The specified storage lifecycle policy does not have any destination with a retention type of **Fixed**.

**Recommended Action:** Verify that the specified storage lifecycle policy has at least one destination that is configured with a **Fixed** retention type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1512

**Message:** storage lifecycle policy must have at least one backup, import, or snapshot operation

**Explanation:** The specified storage lifecycle policy does not have any backup destination.

**Recommended Action:** Verify that the storage lifecycle policy has at least one **Backup** type of destination.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1513

**Message:** invalid priority

**Explanation:** The duplication priority that you specify in the storage lifecycle policy is not valid.

**Recommended Action:** Verify that the duplication priority that you specify in the storage lifecycle policy is in the range of 0 to 99999.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 1514

**Message:** invalid operation type

**Explanation:** The destination type that you specify on one or more destinations in the storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the destination type that you specify on each destination in storage lifecycle policy is either **Backup**, **Duplication**, or **Snapshot**.
- If you are use the `nbstl` command to configure storage lifecycle policy, the following are the valid values for the destination type: 0 indicates **Backup**, 1 indicates **Duplication**, and 2 indicates **Snapshot**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1515

**Message:** Multiplexing value is not valid or cannot be used where specified

**Explanation:** The preserve multiplexing flag that you specify on one or more destinations is not valid.

**Recommended Action:** Do the following, as appropriate:

- If you use the `nbstl` command to configure storage lifecycle policy, then verify that the valid values are used to indicate the preserve multiplexing flag for each destination. The value "T" or "t" indicates true (Preserve multiplexing). The value "F" or "f" indicates false (do not preserve multiplexing).
- Verify that destinations of type **Backup** are not configured to preserve multiplexing.
- Verify that destinations of type **Snapshot** are not configured to preserve multiplexing.
- Verify that destinations of type **Duplication** that are using disk storage units are not configured to preserve multiplexing.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1516

**Message:** all storage units or groups must be on the same media server

**Explanation:** The destinations of type **Backup** specified in storage lifecycle policy are not accessible by the same media server.

**Recommended Action:** Verify that all the destinations of type **Backup** are accessible by at least one common media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1517

**Message:** Invalid retention level

**Explanation:** The retention level that you specify for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Verify that the retention level that you specify on each destination in storage lifecycle policy is in the range of 0 to 100.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1518

**Message:** backup image is not supported by storage lifecycle policy

**Explanation:** The backup image is unsupported by the configured storage lifecycle policy.

**Recommended Action:** Do the following, as appropriate:

- Verify that if a NetBackup policy is configured to perform snapshot backups and uses storage lifecycle policy as its storage destination, then the specified storage lifecycle policy must be configured with a snapshot destination. Otherwise, backup images that are created by those NetBackup policies are not processed further by storage lifecycle policy for any lifecycle operations.
- Verify that NetBackup policies that use the storage lifecycle policy as a storage destination are not configured to perform “snapshots-only” operations. They must create backups in addition to snapshots. The Storage lifecycle policy even though configured with a snapshot destination, performs lifecycle operations on such images only if they have at least one backup copy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1519

**Message:** Images are in process

**Explanation:** The operation in progress cannot complete because the SLP processing of the images is not complete.

**Recommended Action:** Wait until the image processing is done, then retry the operation. Or, terminate the SLP processing for the needed images.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1521

**Message:** Database not available

**Explanation:** The import manager is not able to access the NetBackup database.

**Recommended Action:** Do one of the following:

- Make sure that the database service is running.
- Make sure that the disk is not full.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1522

**Message:** Error executing database query

**Explanation:** An SQL error is in the import manager.

**Recommended Action:** Examine the log files for the `nbstserv` process or originator ID 369 for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1523

**Message:** Invalid fragment

**Explanation:** NetBackup received from a storage device a replication notification event in an unrecognized format.

**Recommended Action:** Check the NetBackup Problems Report for details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1524

**Message:** Duplicate image record

**Explanation:** NetBackup received from a storage device a replication notification event for a backup ID that already exists in the NetBackup catalog.

**Recommended Action:** Do one of the following:

- Check the NetBackup Problems Report for details.
- Delete the duplicate image from storage because NetBackup cannot do it.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1525

**Message:** Invalid lsu

**Explanation:** NetBackup received a replication notification event that indicates an image exists on an unknown or unconfigured disk volume (LSU).

**Recommended Action:** Do one of the following:

- Configure the LSU as a valid disk volume in a valid disk pool, and create a valid storage unit for it. Associate this storage unit with an import storage lifecycle policy.
- Reconfigure the replication on your storage devices to use a replication target disk volume (LSU) that NetBackup recognizes.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1526

**Message:** Storage lifecycle policy exceeds maximum import operations

**Explanation:** The storage lifecycle policy definition cannot be created or modified as specified because it can contain only one import destination.

**Recommended Action:** Configure the storage lifecycle policy with only one import destination.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1527

**Message:** storage lifecycle policy can have only one of backup, import, and snapshot operations

**Explanation:** The storage lifecycle policy definition cannot be created or modified as specified because a storage lifecycle policy with an import destination cannot also have backup or snapshot destinations.

**Recommended Action:** Configure the storage lifecycle policy with only one import destination and additional destinations of type duplication only.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1528

**Message:** The source copy for an Auto Image Replication is not capable of replication

**Explanation:** The storage lifecycle policy (SLP) definition cannot be created or modified as specified because you have selected an Auto Image Replication destination that duplicates a copy not capable of duplication across master servers.

**Recommended Action:** Do one of the following:

- If you use the command line, ensure that you specify the correct SLP destination index number for the source copy.
- Use the appropriate indentation to indicate the correct source storage lifecycle policy destination in the GUI.
- Ensure that the source uses a storage unit that is capable of replication. The storage unit is specified by the SLP destination index on the CLI or by indentation in the GUI. That is, check the properties of the disk volumes within the disk pool that the storage unit specifies.
- After you set a replication target, you must refresh the disk pool. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management Devices > Disk Pools**. In the right pane, select the disk pool that you want to update. In the **Change Disk Pool** dialog box, click **Refresh** to configure the replication settings for the disk pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1529

**Message:** The source copy for Auto Image Replication must specify a storage unit

**Explanation:** One of the following may have occurred:

- The storage lifecycle policy definition cannot be created or modified as specified because an Auto Image Replication destination is specified which duplicates a copy that may not be capable of duplication across master servers.
- You are trying a replication by using a storage unit group. Auto Image Replication does not support replicating from or replicating to a storage unit group. That is, the source copy cannot be in a storage unit group, and the target cannot be a storage unit group.

**Recommended Action:** Do one or more of the following:

- If you use the command line, ensure that you specify the correct storage lifecycle policy destination index number for the source copy.
- Ensure that you use the appropriate indentation to indicate the correct source storage lifecycle policy destination in the GUI.
- Ensure that the source that is specified by either the storage lifecycle policy destination index on the CLI or by indentation in the GUI uses a storage unit (not a storage unit group, storage lifecycle policy or Any Available) that is capable of replication. That is, check the properties of the disk volumes within the disk pool that the storage unit specifies.
- Ensure that you are not using a storage unit group for replication. For the source copy, select a storage unit that is not in a storage unit group. For the target, do not select a storage unit group.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1530

**Message:** Only one Auto Image Replication allowed per copy

**Explanation:** The storage lifecycle policy definition cannot be created or modified as specified because an Auto Image Replication destination is specified which duplicates a copy which already has an Auto Image Replication specifying it as a source copy.

**Recommended Action:** Do one of the following:

- If you use the command line, ensure that you specify the correct storage lifecycle policy destination index number for the source copy.
- Ensure that you use the appropriate indentation to indicate the correct source storage lifecycle policy destination in the GUI.
- Ensure that the source that is specified by either the storage lifecycle policy destination index on the CLI or by indentation in the GUI does not have more than one Auto Image Replication destination specifying it as its source copy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1531

**Message:** An import storage lifecycle policy requires one copy with remote retention type

**Explanation:** The storage lifecycle policy definition cannot be created or modified as specified because an imported image must make at least one copy by using the (imported) remote retention type.

**Recommended Action:** Add a destination to the storage lifecycle policy that uses the remote retention type.

Do one of the following:

- Change one of the destinations in the storage lifecycle policy to use the remote retention type. If the storage lifecycle policy has only one destination that is an import destination, then it must be a remote retention type.
- Add a destination to the storage lifecycle policy which uses the remote retention type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1532

**Message:** Import failed because the imported image specifies an SLP name which does not exist

**Explanation:** The image imported does not match any configured storage lifecycle policy and was immediately expired.

**Recommended Action:** Do one of the following:

- Verify that the storage lifecycle policy in the source domain where you configured an Auto Image Replication matches the storage lifecycle policy in the destination domain where you configured the import. The match is case-sensitive.
- Add a storage lifecycle policy with an import destination using the same name as your storage lifecycle policy in the source domain.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1533

**Message:** Import failed because the imported image data class is different than the SLP data class

**Explanation:** The image that is imported has a data classification which does not match any of the import storage lifecycle policy data classifications and was immediately expired.

**Recommended Action:** Do one of the following:

- Change the data classification of the storage lifecycle policy in the source domain where you configured an Auto Image Replication to match the following: the data classification in the destination domain where you have configured the import. The match is case-sensitive.  
Verify that the storage lifecycle policy in the source domain where you configured an Auto Image Replication matches the following: the storage lifecycle policy in the destination domain where you configured the import. The match is case-sensitive.
- Change the data classification of the storage lifecycle policy in the destination domain where you configured an Auto Image Replication to match the following: the data classification in the source domain where you have configured the import. The match is case-sensitive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1534

**Message:** Import failed because the imported image specifies an SLP name with no import operation

**Explanation:** The imported image specifies a storage lifecycle policy name that is not an import storage lifecycle policy and is immediately expired.

**Recommended Action:** Use a different storage lifecycle policy name in the source domain where you configured an Auto Image Replication. This name must match a storage lifecycle policy name with an import destination in the destination domain where you have configured the import. The match is case-sensitive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1535

**Message:** Import failed because the imported image backup ID conflicts with an existing image



**Explanation:** NetBackup attempted to import an image with a backup ID that already exists in the image catalog.

**Recommended Action:** Delete the duplicate image from storage because NetBackup cannot delete it. Use the following command:

```
# bptime -deletecopy # -backupid backupid
```

where # is the copy number of the image that you want to delete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1536

**Message:** The storage unit or storage unit group cannot be deleted because an SLP references it

**Explanation:** You cannot delete a storage unit or storage unit group if a storage lifecycle policy (SLP) references it. The SLP may be an older version. The **NetBackup Administration Console** displays the most recent version of an SLP while the reference to the storage unit or storage unit group may be located in an earlier version.

**Recommended Action:** Use the `nbstl` command to view and change the older SLP versions. Do the following in the order listed:

- Run the following command to display all versions of each SLP:

```
# nbstl -L -all_versions
```

- Determine the name and version of each SLP that references the storage unit or storage unit group.
- Run the following command to replace the storage unit (group) to be deleted with the name of a different storage unit.

```
# nbstl <SLP_name> -modify_version <version_number>...
```

For more information on storage lifecycle policy versions, see the [NetBackup Administrator's Guide, Volume I](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1537

**Message:** Backup policy and storage lifecycle policy have conflicting configurations

**Explanation:** Some of the backup policy characteristics are not compatible with one of the SLP characteristics that is referenced in the policy attributes or policy schedules.

**Recommended Action:** In the **NetBackup Administration Console**, locate the **Change Storage Lifecycle Policy** dialog for the SLP in question. Then run the Validation Report to display the specific conflicts that pertain to the SLP. Correct those conflicts.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1538

**Message:** Data classification in the SLP conflicts with backup policy

**Explanation:** The Data classification that you specify in the SLP does not match the data classification that is specified in the backup policy.

**Recommended Action:** Do one of the following:

- Change the policy to reference an SLP with a matching data classification
- Change the data classification in either the backup policy or the SLP so that they match.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1539

**Message:** Backup policy generates snapshots but storage lifecycle policy does not handle them

**Explanation:** The backup policy generates snapshots because you have selected the **Perform snapshot backups** and the **Retain snapshot for Instant Recovery or SLP management** on the **Change Policy** dialog box. The referenced SLP cannot process snapshots because it does not include a Snapshot operation.

**Recommended Action:** Do one of the following:

- Change the backup policy to use an SLP that provides snapshot support.
- Change the backup policy so it does not generate snapshots.
- Change the SLP to include a snapshot operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1540

**Message:** SLP expects snapshots but backup policy does not create them with SLP management enabled

**Explanation:** The maximum snapshot limit for this policy is reached and no existing snapshot is eligible for rotation.

**Recommended Action:** Find and expire the existing snapshot which is no longer needed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1541

**Message:** Snapshot creation failed. The maximum snapshot limit for the policy has been exceeded and no existing snapshots are eligible for expiration.

**Explanation:** One of the following is true:

- None of the existing snapshot copies is eligible for expiration because all the copies are in snapshot duplication pending mode.
- None of the existing snapshot copies is eligible for expiration, because they have not yet reached their retention period (fixed retention).

**Recommended Action:** Do not try to expire a snapshot copy that is still pending or has not reached its retention period. Check the maximum snapshot limit setting in your **Backup Policy>Attributes>Snapshot Options**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1542

**Message:** An existing snapshot is no longer valid and cannot be mounted for subsequent operations

**Explanation:** An existing snapshot has become corrupted or the snapshot no longer contains all the required data. It cannot be mounted and cannot be used for any further NetBackup operations, including backup from snapshot or restore. Any pending SLP operations have been automatically canceled

**Recommended Action:** Run a new backup job to generate a new snapshot.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1543

**Message:** Policy type is not compatible with SLP operations

**Explanation:** Policies of the type that you specify cannot be used with the referenced SLP because they do not support the SLP operations, including SLP characteristics such as snapshot operations.

**Recommended Action:** Choose a different SLP that is compatible with the policy type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1545

**Message:** Schedule type is not compatible with SLP operations

**Explanation:** A policy schedule refers to an SLP as its storage destination, but the schedule type is not compatible with the operations performed by the SLP.

**Recommended Action:** Choose a different SLP that is compatible with the schedule type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1546

**Message:** Capacity managed retention type is not compatible with SLP operations

**Explanation:** Capacity managed retention has been chosen as the retention type for an SLP operation. That retention type does not support the SLP operations.

**Recommended Action:** Choose a different SLP that is compatible with the schedule type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1547

**Message:** Expire after copy retention requires a dependent copy

**Explanation:** When the retention type for an SLP operation is **expire after copy**, a dependent copy for that operation must use the **expire after copy** operation as its source.

**Recommended Action:** No operations can be performed on this snapshot. Expire it from the catalog.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1548

**Message:** Retention type is not compatible with snapshot operation

**Explanation:** The retention type that you selected for the snapshot operation in an SLP is not supported for snapshots.

Possible scenario: You configure the backup policy for Replication Director, and in the **Attributes** tab you select **Any Available** for the **Policy storage**. In the schedule for the backup policy, you select **Override policy storage selection** and select an SLP from the drop-down menu. The SLP contains a storage unit that uses a **Fixed** retention type. The backup policy validation fails and asks you to set the **Maximum Snapshot Limit** to **Managed by SLP Retention**.

**Recommended Action:** Do one of the following:

- Choose a different retention type.
- If the backup policy is configured for Replication Director, open the backup policy. In the **Attributes** tab, click **Options** to display the Replication Director options. If the values for the **Maximum Snapshots** do not include **Managed by SLP Retention**, select 0 (zero) instead. A value of 0 indicates the **Managed by SLP Retention** selection.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1549

**Message:** TIR information selection is not compatible with SLP operations

**Explanation:** The backup policy has TIR information collection that is enabled and uses an SLP as its storage destination. One or more of the operations in the SLP do not support TIR information collection.

**Recommended Action:** Do one of the following:

- Remove the TIR information selection from the backup policy.
- Choose a different SLP to use with the backup policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1552

**Message:** The source and target storage units are not valid replication partners.

**Explanation:** The `nbstl` command has configured the lifecycle policy. One of the following is true:

- The target storage unit or group that is specified for the replication operation is not a replication partner for the source storage unit or group.
- Volumes that are configured in the target storage unit or group are not replication targets for the volumes that are configured in the source storage unit or group.
- You use the fully qualified name for the storage server. The storage server creation process requires the short version of the name as displayed in the `bpstsinfo -li` output.

**Recommended Action:** Do one of the following:

- Run the following command to get a list of matching target storage units or groups for the given source storage unit or group:

```
# nbdevquery -listreptargets -stunit source_stu_or_group
```

- Rerun the `nbstl` command with the target storage unit or group from the list that the `nbdevquery` command displays.
- Run the `bpstsinfo -li` command and check the output for the storage server name. The name that you use to create the storage server must match this name.
- Ensure that NetBackup is configured after the storage server configuration is complete. If not, use the **Change Disk Pool** dialog of the **NetBackup Administration Console** or the `nbdevconfig -updatedp` command to refresh each disk pool of the storage server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1553

**Message:** Checkpoints are not allowed with SLP operations

**Explanation:** The backup policy has checkpoint restart capability enabled and uses an SLP as its storage destination. The SLP contains one or more operations that do not support checkpoint restart.

**Recommended Action:** Do one of the following:

- Remove the checkpoint restart selection from the backup policy.

- Choose a different SLP to use with the backup policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1554

**Message:** Storage unit snapshot capability is not compatible with operation characteristics

**Explanation:** The snapshot capability of a storage unit does not support the SLP operation that uses it.

**Recommended Action:** Choose a storage unit that supports the correct capabilities.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1556

**Message:** The SLP deletion failed because a backup policy refers to it.

**Explanation:** An attempt to delete an SLP has failed because the SLP is still referenced in one or more backup policies.

**Recommended Action:** Change the backup policies to use other SLPs or storage units. Then try again to delete the SLP.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1557

**Message:** Must specify mirror retention when target storage unit is mirror capable.

**Explanation:** You have specified a target storage unit that is mirror-capable for a replication operation in a storage lifecycle policy, but the retention is not mirror type.

**Recommended Action:** If you used a `nbsl` command to configure the storage lifecycle policy, rerun the command after the following: Specify the mirror retention type for the replication operation corresponding to the storage unit that is mirror-capable. Use the `bpsl` command to view the storage unit properties. If the error occurs when you configure the storage lifecycle policy by using the GUI, submit a problem report and provide the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1558

**Message:** Mirror retention is not allowed when target storage unit is not mirror capable.

**Explanation:** When you configured the replication operation in a storage lifecycle policy, you specified a mirror retention for a target storage unit that is not mirror-capable.

**Recommended Action:** If you used a `nbstl` command to configure the storage lifecycle policy, rerun the command after you do the following: Specify the appropriate retention type (other than mirror retention) for the replication operation corresponding to the storage unit that is non-mirror capable. Use the `bpstulist -u` command to view the storage unit properties. If the error occurs when you configure the storage lifecycle policy by using the GUI, submit a problem report and provide the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1559

**Message:** SLP referenced in policy or schedule not found

**Explanation:** The SLP named in the attributes of a backup policy or in one of the policy schedules cannot be found.

**Recommended Action:** Check the spelling of the SLP used in the policy. The SLP displayed in the **NetBackup Administration Console** or the `nbstl` command can be used to list the SLPs that have been defined. Select one of the defined SLPs to use in the backup policy or create one with the desired name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1560

**Message:** Fixed or rotation retention required without a replication operation

**Explanation:** An SLP that contains an Auto Image Replication operation must contain at least one operation with a **Fixed Snapshots** or **Maximum Snapshots** retention type.

**Recommended Action:** Add an operation with the required retention or change the retention of an existing operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 1561

**Message:** Policy using NDMP conflicts with multiple **Backup From Snapshot** operations in storage lifecycle policy

**Explanation:** If the backup policy uses NDMP through either the policy type or the data mover type, it cannot use an SLP that contains multiple **Backup From Snapshot** operations.

**Recommended Action:** Do one of the following:

- Change the policy type or data mover type so that it is not NDMP.
- Use a different SLP that does not contain multiple **Backup From Snapshot** operations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1562

**Message:** Backup schedule generates snapshots but storage lifecycle policy does not handle them

**Explanation:** A backup policy schedule generates snapshots but the SLP that is referenced by that schedule does not contain a **Snapshot** operation. Thus, the SLP cannot process snapshots.

**Recommended Action:** Select an SLP that begins with a Snapshot operation so that it can process the snapshot generated by the backup policy and schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1563

**Message:** SLP expects snapshots but backup schedule does not create them

**Explanation:** A backup policy schedule refers to an SLP that starts with a Snapshot operation and expects to process snapshots. The backup policy and the relevant schedule do not generate snapshots.

**Recommended Action:** Select an SLP that does not begin with a **Snapshot** operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1564

**Message:** Storage lifecycle policy contains errors

**Explanation:** NetBackup calls the SLP validation functions in `bpdbm`. Other error status values are returned.

**Recommended Action:** Check the other errors that are displayed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1565

**Message:** Policy snapshot method is not compatible with SLP snapshot operations

**Explanation:** The snapshot method chosen in the backup policy does not provide support for the snapshot operations defined in the referenced SLP.

**Recommended Action:** Use a different SLP that does not contain unsupported operations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1566

**Message:** Storage unit required for snapshot operation when no other operation present

**Explanation:** NetBackup can determine which storage unit to use for a **Snapshot** operation if there are other operations in the SLP. If the **Snapshot** operation is the only operation in the SLP, a storage unit must be provided.

**Recommended Action:** Add a storage unit to the **Snapshot** operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1567

**Message:** Only one NDMP backup of a snapshot per backup ID is allowed

**Explanation:** A backup policy of type NDMP refers to an SLP that contains more than one Backup From Snapshot operation.

**Recommended Action:** Do one of the following:

- Modify the SLP so that it contains only one Backup From Snapshot operation.
- Modify the backup policy so that it uses a different SLP.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1568

**Message:** Only one **Index From Snapshot** operation is allowed per storage lifecycle policy

**Explanation:** You have defined an SLP that contains more than one **Index From Snapshot** operation. Only one **Index From Snapshot** operation is allowed in an SLP.

**Recommended Action:** Change the backup policies to use other SLPs or storage units. Then try again to delete the SLP.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1569

**Message:** Snapshot storage unit is not configured for primary snapshots. It cannot be used in snapshot operation.

**Explanation:** A snapshot-capable storage unit must be configured to handle primary snapshots if you want to use a **Snapshot** operation in an SLP.

**Recommended Action:** Do one of the following:

- Select a different storage unit that is snapshot-capable to use in the **Snapshot** operation.
- Change the configuration of the desired storage unit so that it supports primary snapshot operations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1570

**Message:** Policy type does not support **Index from Snapshot**

**Explanation:** The backup policy type does not support **Index from Snapshot** operations. The SLP referenced by the policy contains an **Index from Snapshot** operation

**Recommended Action:** Select a different SLP that does not contain an **Index from Snapshot** operation

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1571

**Message:** Data mover type specified in policy does not support **Index from Snapshot**

**Explanation:** The data mover type selected in the backup policy does not support **Index from Snapshot** operations. The SLP referenced by the policy contains an **Index from Snapshot** operation.

**Recommended Action:** Select a different SLP that does not contain an **Index from Snapshot** operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1572

**Message:** Storage unit must be specified for this operation

**Explanation:** An SLP operation has been defined but no storage unit has been included in the operation. Other than **Snapshot** operations in some circumstances, all SLP operations require a storage unit to be defined.

**Recommended Action:** Add a storage unit to the SLP operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1573

**Message:** Backup image cannot be expired because its SLP processing is not yet complete

**Explanation:** You tried to expire one or more copies of an SLP-managed image. The SLP processing that depends on those copies is not complete. The image cannot be expired.

**Recommended Action:** Do one of the following:

- Wait until SLP processing for that image is complete, then retry the expiration operation.
- Use the `nbslutil -cancel` command to cancel further processing on the relevant image. Then retry the expiration operation.

- Add the `-force_not_complete` option to the `bpexpdate` command to force expiration even if the image-copy is not SLP complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1574

**Message:** Data Classification name cannot be 'Any' while creating new data classification

**Explanation:** You cannot use 'Any' as the data classification name when you create a new data classification.

**Recommended Action:** Use a different name and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1575

**Message:** Data Classification auto creation failed

**Explanation:** You are automatically creating a new data classification that is the same as the data classification of the image that is being imported. The data classification of the image should reside on the master server where the image is being imported.

**Recommended Action:** Manually create the data classification on the master server with the same name as that of the image being imported.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1576

**Message:** Topology validation failed

**Explanation:** The validation of the SLP topology fails.

**Recommended Action:** Do the following:

- Check that the media servers that are associated with the storage servers are running.
- Check the connectivity between the media server (or client) and the storage server (NetApp OnCommand server).
- Check the detailed messages supplied with this error to determine the vendor-specific errors.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1577

**Message:** Storage unit in the SLP does not match the accelerator attribute in policy

**Explanation:** The storage unit you have selected for the SLP does not support the accelerator backup.

**Recommended Action:** Select a different storage unit for the SLP that does support the accelerator backup operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1578

**Message:** Invalid window close options

**Explanation:** The window close option is not valid for the SLP operation.

**Recommended Action:** If you used the `nbstl -wcopt` command, make sure that the specified argument is either SFN or SHN.

For more information on the `nbstl` command, please see the [NetBackup Commands Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1579

**Message:** One or more images were not processed because the window closed

**Explanation:** The processing window closes before all the images are processed. The remaining unprocessed images are processed when the window reopens.

**Recommended Action:** This behavior is expected and no action is necessary. Processing resumes when the next window opens.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1580

**Message:** VMware policy with PFI enabled requires an SLP

**Explanation:** When the 'Persistent Frozen Image' is enabled for a VMware policy, Replication Director protects the virtual machines. This policy configuration requires an SLP. This error message is shown at policy validation time.

**Recommended Action:** Use the VMware policy without Replication Director, or provide an SLP that has at least a Snapshot operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1581

**Message:** Non-application consistent VMware policy is not compatible with snapdupe operations

**Explanation:** Backup for Snapshot operations are not supported on Replication Director based VMware policies when Application Consistency is disabled. This error message is shown at policy validation time.

**Recommended Action:** Enable Application Consistency, or remove the Backup from Snapshot operation from the SLP definition.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1582

**Message:** Application consistent VMware policy requires VM quiesce

**Explanation:** Replication Director based VMware policies require that when Application Consistency is enabled, the virtual machines are quiesced. This error message is shown at policy validation time.

**Recommended Action:** Disable Application Consistency or enable virtual machine quiesce.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1583

**Message:** VMware policy with PFI enabled requires VIP auto discovery

**Explanation:** Persistent Frozen Image Replication Director based VMware policies require automatic discovery of virtual machines. The manual selection of virtual machines is not supported. You can select automatic discovery in the **NetBackup Administration Console**. The user can change the setting by using the CLI, but policy validation detects it and generates this error message.

**Recommended Action:** Enable automatic discovery of virtual machines.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1584

**Message:** VMware policy with 'Persistent Frozen Image' enabled requires schedule type of Full Backup

**Explanation:** Replication Director based VMware policies support only full schedule at this time.

**Recommended Action:** Use a full schedule and remove all incremental schedules.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1585

**Message:** Backup image cannot be expired because not all dependent copies are expired

**Explanation:** Other images in the NetBackup catalog are dependent upon the image that is currently being requested for expiration. The selected image cannot be expired at this time. Regular catalog cleanup and expiration operations handle this properly. The dependent images are expired first. But if they are still in SLP processing, they cannot be expired, and therefore the selected image cannot be expired.

**Recommended Action:** Wait for the dependent images to be eligible for expiration when their SLP state transitions into IMAGE\_COMPLETE state. Also, you can cancel the SLP operations on the dependent images.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1586

**Message:** SLP operation was canceled

**Explanation:** You cancel a running SLP operation, and someone else tries to validate the copy.

**Recommended Action:** No action is required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 1587

**Message:** Storage lifecycle policy cannot have both target and untarget replication to remote master

**Explanation:** Do not define the SLP with a combination of a targeted replication operation and an untargeted replication operation.

**Recommended Action:** Do not mix the targeted and untargeted replication operation to a remote master.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1588

**Message:** Target master server is already used in one of the replications to remote master

**Explanation:**

**Recommended Action:** Define all targeted replication operations with distinct target master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1589

**Message:** Cannot connect to specified target master server

**Explanation:** All services must be up and running on source domain as well as target domain.

**Recommended Action:** Check that all services on source domain and target domain are running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1590

**Message:** Cannot find specified target import SLP

**Explanation:** This error generally occurs when you run the `nbstl` command.

**Recommended Action:** Enter a valid name of the target domain SLP with the import operation, in the targeted replication operation of the source domain's SLP.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1591

**Message:** No import SLP(s) found with compatible replication target device.

**Explanation:** In the target domain, the import SLP is present, but the replication target device is not compatible.

**Recommended Action:** Correct one or more of the possible problems.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1592

**Message:** Trusted master servers are being referred by one or more Storage Lifecycle Policies (SLPs) on the source or target domain.

**Explanation:** The user tries to delete a trusted master server from a system. For example, when the user configures Targeted Auto Image Replication between domain A (source domain) and domain B (target domain), domain B must be identified as a trusted master server in domain A. The SLPs are configured to replicate images from domain A to domain B. If the user tries to delete domain A's trusted master entry for domain B when the SLPs still refer to domain B, you will receive this error code.

**Recommended Action:** Delete or change the SLPs so they do not refer to domain B, then try to delete domain B from domain A again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1593

**Message:** Replication Director for VMware policy requires mapped backups

**Explanation:** Replication Director based VMware policies support individual files and folders recovery for all the protection virtual machines. Therefore, the virtual machine mapping is selected automatically in the **NetBackup Administration Console**. The user can change its setting by using the CLI, but policy validation detects it and generates this error message.

**Recommended Action:** Enable mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1594

**Message:** Failed to determine disk media ID

**Explanation:** While importing the image in the target domain, the operation could not determine the disk media ID. The storage server, disk pool, and storage unit must each have a valid configuration.

**Recommended Action:** Recheck the storage server, disk pool, and storage unit configurations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1596

**Message:** Select a storage lifecycle policy that has no snapshot operation as a policy's Storage Destination

**Explanation:** Standard storage unit or a storage lifecycle policy that has no snapshot operation is expected as a policy's storage destination.

**Recommended Action:** Select a storage lifecycle policy that has no snapshot operation as the policy storage destination.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1597

**Message:** Replication Director for Oracle policy requires an SLP

**Explanation:** If you select **Use Replication Director** on an Oracle policy, you must specify a snapshot SLP as the Override policy storage selection on the full schedule.

**Recommended Action:** Configure an SLP with a Snapshot as the first operation and Replication as a subsequent operation. Specify this SLP as the Override policy storage selection on the Full schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1598

**Message:** Oracle policy with PFI and FI enabled requires an SLP

**Explanation:** If you select **Perform snapshot backups** and **Retain snapshot for Instant Recovery or SLP management** on an Oracle policy, you must set up an SLP as the Override policy storage selection on the full schedule.

**Recommended Action:** Configure an SLP with a Snapshot as the first operation. Specify this SLP as the Override policy storage selection on the Full schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1599

**Message:** Application schedule storage selection cannot be a snapshot SLP

**Explanation:** You have specified An SLP with Snapshot as the first action for the Override policy storage selection on the Application schedule.

**Recommended Action:** Specify a non-SLP storage (basic disk, tape, advanced disk, etc.) or an SLP with Backup as the first operation for an Override policy storage selection on the Application schedule

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1600

**Message:** The Policy storage is a snapshot SLP and the Application schedule does not override the policy storage selection. Snapshot SLP storage is not allowed on an Application schedule.

**Explanation:** You have selected an SLP with Snapshot as the first operation for the Policy storage in the Attributes tab and the Application schedule does not override the Policy storage.

**Recommended Action:** Specify a non-SLP storage (basic disk, tape, advanced disk, etc.) or an SLP with Backup as the first operation for the Policy storage or as the Override policy storage selection on the Application schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1601

**Message:** Full schedule requires a snapshot SLP

**Explanation:** The current policy configuration requires a snapshot SLP as the Override policy storage selection on the Full schedule.

**Recommended Action:** Configure an SLP with a Snapshot as the first operation. Specify this SLP as the Override policy storage selection on the Full schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1602

**Message:** The Policy storage is not a snapshot SLP and the Full schedule does not override the policy storage selection. Snapshot SLP storage is required on the Full schedule.

**Explanation:** You have specified an SLP with Backup as the first operation for the policy storage in the Attributes tab and the Full schedule does not override the policy storage.

**Recommended Action:** Specify either an SLP with a Snapshot as the first operation for the Policy storage or as the Override policy storage selection on the Full schedule.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1603

**Message:** Failed to save target SLP volume information

**Explanation:** This error occurs internally when NetBackup tries to create a storage lifecycle policy with the targeted replication operation. While it configures the replication operation, it caches the selected target domain SLP volume information in the EMM of the source domain. If the caching fails, it logs an appropriate message in the `nbemm` logs.

**Recommended Action:** Take action as dictated by the EMM logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1604

**Message:** No import SLP(s) found with compatible data class.

**Explanation:** No import SLP is found with a compatible data classification or the target has no import SLP at all.

**Recommended Action:**

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1800

**Message:** Invalid client list

**Explanation:** For Enterprise Vault-type policies, verify that multiple clients are not added to the list of clients if you specify any of the following Enterprise Vault 8.0 directives in the backup selection:

- EV\_INDEX\_LOCATION=
- EV\_VAULT\_STORE\_DB=
- EV\_OPEN\_PARTITION=
- EV\_CLOSED\_PARTITIONS=
- EV\_FINGERPRINT\_DB=
- EV\_READY\_PARTITIONS=

**Recommended Action:** Specify only one client in the policy, or remove the directive from the backup selection that does not support multiple client.

See the Troubleshooting section of the [NetBackup for Enterprise Vault Agent Administrator's Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1915

**Message:** Cannot delete instance group that contains instances (delete or move instances first)

**Explanation:** User tries to delete an instance group that contains instances.

**Recommended Action:** First delete the instances individually by selecting them under the instances node in the **NetBackup Administration Console** or by using the `nboraadm -delete_instances`. After all the instances in the group have been deleted, try again to delete the group.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1916

**Message:** Database error, cannot access the instance repository

**Explanation:** The user tries to view the list of instances in the **NetBackup Administration Console**, but the Sybase database is down.

**Recommended Action:** Make sure that all NetBackup services are started and that `nbbd` installed correctly.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1917

**Message:** Cannot add instance group, this group name is already in use

**Explanation:** User tries to add an instance group with the same name as an existing group. All instance groups must have unique names.

**Recommended Action:** Do one of the following:

- CLI: Retry the `nboraadm -add_instance_group` command again with a different group name.
- GUI: Type a different group name in the appropriate field, and try to add the group again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1918

**Message:** Cannot find a group by this name

**Explanation:** The user tries to delete or modify an instance group that does not exist. If this error occurs on the command line, the group name may be spelled incorrectly. Because of the cache in the **NetBackup Administration Console**, an instance group name may yet appear in the list of instance groups even though the group does not exist anymore.

**Recommended Action:** Do one of the following:

- CLI: Make sure that the group name is spelled correctly. Note that group names are case-sensitive. If you believe that the name is correct, run `nboraadm -list_instance_groups` to verify what groups exist.
- GUI: Refresh the view (`F5` key).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1919

**Message:** This instance or instance group was modified by another process, refresh before editing

**Explanation:** In the **NetBackup Administration Console**, the user tries to edit, modify, or delete an instance or instance group that another process has modified.

**Recommended Action:** Refresh the view (F5 key).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1920

**Message:** An instance with this name and client already exists

**Explanation:** A user tries to add an instance whose name already exists in the repository (ORACLE SID), client, and home directory. These three identifiers make an instance unique, so at least one must be changed to add another instance.

In the GUI, a user tries to add a new instance to an unrefreshed display, so they try to add it again.

**Recommended Action:** Do one of the following:

- CLI: Use `nboraadm -list_instances` to view the instances that already exist.
- GUI: Refresh the view (F5 key).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1921

**Message:** The specified instance cannot be found

**Explanation:** The user tries to modify or delete an instance that does not exist.

**Recommended Action:** Do one of the following:

- CLI: Make sure that the instance name is spelled correctly, because you specify the instance by typing the instance name (ORACLE SID). On Windows, the instance name is not case-sensitive. On UNIX, the instance name is case-sensitive
- GUI: Refresh the view (F5 key).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1922

An instance with this name/client is already registered



**Explanation:** A user tries to register a duplicate instance. An instance with the same name, client, and home directory has already been registered in the repository (ORACLE SID). These three identifiers make an instance unique, so at least one identifier must be changed to register another instance.

**Recommended Action:** Do one of the following:

- CLI: Run `nboraadm -list_instances` to view what instances already exist.
- GUI: Refresh the view (F5 key).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1924

**Message:** Domain is a required field for Windows instances

**Explanation:** The user tries to register a Windows instance, but a domain is not specified.

**Recommended Action:** Specify a domain in the domain field, then try to register the instance again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1925

**Message:** The requested operation(s) failed

**Explanation:** A generic, unspecified error occurred. Different versions of NetBackup may exist on the client and the server. Or, you ran the `nboraadm` command with the wrong parameters.

**Recommended Action:** Recheck the command line arguments. If the error persists, check the debug logs for clues or contact Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1926

**Message:** The entry specified already exists

**Explanation:** The user tries to add a database administrator by running `nboraadm`, but that user has already been added. A user name and a client name make a unique entry.

**Recommended Action:** The DBA has already been added, so no action is needed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1927

**Message:** The entry specified does not exist

**Explanation:** The user tries to add a database administrator using `nboraaadm`, but that user does not exist in the DBA list.

**Recommended Action:** The user has already been deleted, so no action is likely needed. Use the `nbboraadm -list_dbas` command to verify the list of DBAs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 1928

**Message:** The credentials for 1 or more instances could not be verified

**Explanation:** The validation failed. No specific information has returned that explains the reason why. The user name or password may be incorrect, or an issue exists connecting to the client.

**Recommended Action:** Make sure that the client is running at least this version of NetBackup, and is configured to use the correct master server. Make sure that you correctly entered the user name, password, and auxiliary fields such as domain (Windows) or TNS (Oracle or RMAN).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2000

**Message:** Unable to allocate new media for backup, storage unit has none available.

**Explanation:** The NetBackup Media and Device Selection component (MDS) did not allocate a new tape volume for backups. The storage unit has no more volumes available in the volume pool for this backup. NetBackup does not change storage units during the backup.

**Recommended Action:** Try the following:

- Check the NetBackup Problems report to determine the storage unit that is out of media.
- If the storage unit is a robot with empty slots, add more volumes and specify the correct volume pool. If no empty slots exist, move some media to non-robotic

and add new volumes. If you have difficulty keeping track of your available volumes, try the `available_media` script located in the following directory:

On UNIX: `/usr/opensv/netbackup/bin/goodies/available_media`

On Windows: `install_path\NetBackup\bin\goodies\available_media.cmd`

This script lists all volumes in the volume configuration, and information on the volumes currently assigned to NetBackup.

- Set up a scratch volume pool as a reserve of unassigned tapes. If NetBackup needs a new tape and none are available in the current volume pool, it moves a tape from the scratch pool into the volume pool that the backup uses.
- If the storage unit and volume pool appear to have media, verify the following:
  - Use the NetBackup Media List report to check if the volume is FROZEN or SUSPENDED. If so, use the `bpmedia` command to unfreeze it or unsuspend it, if so desired.
  - The volume has not expired or exceeded its maximum number of mounts.
  - The EMM database host name for the device is correct. If you change the EMM database host name, stop and restart the Media Manager device daemon (`ltid` for a UNIX server) or the NetBackup Device Manager service (Windows server).
  - The correct host is specified for the storage unit in the NetBackup configuration. The host connection must be the server (master or media) with drives connected to it.
  - The Media and Device Management volume configuration has media in the correct volume pool. Unassigned or active media is available at the required retention level. Use the NetBackup Media List report to show the retention levels, volume pools, and status for all volumes. Use the NetBackup Media Summary report to check for active volumes at the correct retention levels.
- Create the `bptm` debug log directory, and set the MDS VxUL logging (OID 143) to debug level 2. Then retry the operation.
- If this storage unit is new and this attempt to use it is the first, stop and restart NetBackup on the master server. The MDS unified logging files (OID 143) at debug level 2 usually show the NetBackup media selection process.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2001

**Message:** No drives are available for this job

**Explanation:** A job requested a tape drive, but no eligible drive path was configured for the job.

**Recommended Action:** Try the following:

- Verify that the required drives and robots are configured and up.
- Verify that `ltid` is active and a drive path exists that is configured on the drive for the media server that the storage unit requires.
- If the job requires an NDMP drive path, verify that one exists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2002

**Message:** Invalid STU identifier type

**Explanation:** A job has asked for allocation using an invalid storage unit identifier type. The only valid storage unit identifier types are 0 (specific STU), 1 (group) or 2 (ANY).

**Recommended Action:** This error is internal. Call NetBackup support for resolution.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2003

**Message:** Drive is not allocated.

**Explanation:** MDS has been asked to deallocate a drive that is not allocated.

**Recommended Action:** This error is internal to the MDS component of NetBackup.

Check the following logs:

- The MDS unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2004

**Message:** Drive is already allocated

**Explanation:** MDS has been erroneously asked to allocate a drive that is already allocated.

**Recommended Action:** A drive may have been reset while it was allocated for a job. Wait for the jobs that use the drive to complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2005

**Message:** MDS has received an invalid message from a media server.

**Explanation:** `bptm` or `bpdm` on a media server has sent an improperly formatted message to MDS.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
- The `bptm` legacy log from the media server, with `VERBOSE=5`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2006

**Message:** NDMP credentials are not defined in EMM.

**Explanation:** No eligible media server is configured with NDMP credentials to access the NDMP storage unit. Or, NetBackup tried to restore an NDMP image from a disk storage unit when the media server does not have a valid version of NetBackup.

**Recommended Action:** If the job uses an NDMP device, verify that the media server has NDMP credentials that are configured for the filer.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2007

**Message:** Storage unit is not compatible with requesting job

**Explanation:** A job has asked for a storage unit that cannot be used for the job.

**Recommended Action:** A job tries to run on a media server that is running an older version of NetBackup. The job may require a feature that is not available on the media server being requested. Verify that the storage unit type and the media server that the policy and storage unit call out support the feature.

This error can occur when the policy being run is not compatible with the storage units requested by the policy:

- Catalog backups are directed to shared disk storage units.
- Multiplexed jobs are directed to storage units that do not have the multiplex feature configured.
- NDMP backup policies are directed to non-NDMP storage units.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2008

**Message:** All compatible drive paths are down

**Explanation:** All configured drives that can be used for this job are down.

**Recommended Action:** Verify that `ltid` is running on the required media server, and that the media server is active for tape. Using a device monitor, bring up the drive paths if they are down. If the drives are downed again, clean the drives.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2009

**Message:** All compatible drive paths are down but media is available

**Explanation:** All configured drives that can be used for this job are down.

**Recommended Action:** Verify that `ltid` is running on the required media server, and that the media server is active for tape. Using a device monitor, bring up the drive paths if they are down. If the drives are downed again, clean the drives.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2010

**Message:** Job type is invalid

**Explanation:** The job type that is specified in an allocation request to the Resource Broker is not valid for the operation requested.

**Recommended Action:** This error is internal. Call NetBackup Technical Support if this error causes jobs to fail.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2011

**Message:** The media server reported a system error

**Explanation:** An allocation for the media server is in an inconsistent state.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2012

**Message:** Media has conflicts in EMM

**Explanation:** You cannot use the requested media because it is marked as having conflicts in the `nbemm` database.

**Recommended Action:** The media is marked as having conflicts. The upgrade from NetBackup 5.x has found multiple volume databases where two tapes in different volume databases have the same media ID. Call Technical Support to resolve this situation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2013

**Message:** Error record insert failed

**Explanation:** A database record insert has failed.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2014

**Message:** Media is not assigned

**Explanation:** A job requires assigned media, but the requested media is not assigned.

**Recommended Action:** Verify that the job requested the desired media. For example, if you want to list contents of the media, make sure that you have specified the correct media ID.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 2015

**Message:** Media is expired

**Explanation:** A job is trying to write to media that has already expired.

**Recommended Action:** Make sure that non-expired media is available for the job.

Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2016

**Message:** Media is assigned to another server

**Explanation:** A job cannot use the media on the storage server, because the media is assigned to another storage server.

**Recommended Action:** Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2017

**Message:** Media needs to be unmounted from a drive

**Explanation:** The requested media needs to be unmounted from the drive it is in before it can be used for another job.

**Recommended Action:** Identify the media that is requested by the job that returns this error. If it is used by another job, wait for that job to complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2018

**Message:** Number of cleanings is invalid

**Explanation:** A cleaning media has an invalid number of cleanings that remain.

**Recommended Action:** On the **Change Media** screen, set the number of cleanings remaining for the cleaning media to a number greater than or equal to zero (0).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2019

**Message:** Media is in a drive that is not configured on local system

**Explanation:** A job is configured to use a media volume that has no drive path configured to an eligible media server for the job. A media volume is misplaced or all drive paths are down for the media server accessible by the storage unit that is configured for a job.

**Recommended Action:** If drive paths are down, identify the media server that is configured for use by the storage unit, and bring up the drive path to that media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2020

**Message:** Robotic library is down on server

**Explanation:** NetBackup has marked the robot as down for the required media server.

**Recommended Action:** Verify that the media server that is required for this allocation is running, and verify that `ltid` is up on that media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2021

**Message:** Allocation record insert failed

**Explanation:** The NetBackup `mds` component was unable to update the database for a device allocation.

**Recommended Action:** This error is internal. Check the following logs:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2022

**Message:** Allocation status record insert failed

**Explanation:** The NetBackup `mds` component was unable to update the database with device allocation status information.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2023

**Message:** Allocation identifier is not known to EMM

**Explanation:** The NetBackup `mds` component cannot find the device allocation record that is needed to allocate the device for this job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2024

**Message:** Allocation request update failed

**Explanation:** The NetBackup `mds` component was unable to update the database for a device allocation.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2025

**Message:** Allocation request delete failed

**Explanation:** The NetBackup `mds` component was unable to delete a device allocation from the database.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2026

**Message:** Allocation status request delete failed

**Explanation:** The NetBackup `mds` component was unable to modify an allocation status record for this job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2027

**Message:** Media server is not active

**Explanation:** This job requires a media server that is not currently available.

**Recommended Action:** Do one or more of the following:

- Verify that the media server that is required for this allocation is running.
- If this is a tape job, verify that `ltid` is running on the media server. If a media server has gone offline and returned online, a delay of several minutes may occur before a job can use that media server.
- Use the `vmoprcmd` command to show the state of the media server. If the job is trying to access a disk storage unit, verify that the `nbrmms` process is running on the media server. If the job is trying to access a tape storage unit, verify that `ltid` is running on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2028

**Message:** Media is reserved

**Explanation:** The NetBackup `mds` component cannot allocate media because another job has that media exclusively reserved.

**Recommended Action:** If multiple duplication jobs attempt to use the same tape media for read, each job reserves the media. NetBackup should allow more than one job to get a reservation for the tape media.

This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2029

**Message:** EMM database is inconsistent

**Explanation:** An inconsistency in the NetBackup database prevents allocations for this job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Run the `nbrbutil -resetall` command to get the NetBackup allocation database back into a consistent state. Note that this command cancels all jobs including those that are currently running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2030

**Message:** Insufficient disk space or high water mark would be exceeded

**Explanation:** Insufficient disk space is available to run this job.

**Recommended Action:** Try the following possible solutions:

- If there are images on the disk that can be expired, expire them, and run `nbdelete` to delete the images from disk.
- It may be that NetBackup creates disk images more quickly than they expire. If so, modifications to policies may be necessary to change the rate of image creation and expiration for the disk.
- It may be helpful to lower the high water mark and low water mark for the disk group.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2031

**Message:** Media is not defined in EMM

**Explanation:** The media that is required for this job is not defined in the EMM database.

**Recommended Action:** A media volume that is required for a restore job has been deleted from the EMM database. If the media is available, use `bpimport` to import it.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2032

**Message:** Media is in use according to EMM

**Explanation:** The NetBackup database indicates that the media is in use but is not allocated to another job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2033

**Message:** Media has been misplaced

**Explanation:** Job requires media that is not in the expected robotic slot.

**Recommended Action:** Verify that the media that is required by the job is in the proper robotic slot as shown by `vmquery`.

If the error persists, the following logs may be useful in understanding the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
- The verbose `bptm` logs on the media server(s) that access this media.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2034

**Message:** Retry the allocation request later

**Explanation:** Resources that are required for a job are currently in use.

**Recommended Action:** This error should never appear as a job return status. In the `mds` and `nbrb vxul` logs, it indicates that a job should queue because resources are busy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2035

**Message:** Request needs to pend

**Explanation:** A job requires operator intervention before it can continue.

**Recommended Action:** This error should never appear as a job return status. In the `mds` and `nbrb vxul` logs, it indicates that a job should post a request for operator intervention to the NetBackup device monitor.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2036

**Message:** Drive is in a robotic library that is up

**Explanation:** Operator has attempted to assign a pending tape mount request to a drive that is in a robot that is up.

**Recommended Action:** A request for non-robotic media may have caused a pending request in the device monitor, and the operator has assigned the request to a drive that is not a standalone drive. This error is not fatal. The request will pend again in the NetBackup device monitor. Assign the pending mount to a standalone drive or to a drive that is in AVR mode (non-robotic).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2037

**Message:** Drive is not ready

**Explanation:** The required tape is in a drive, but the drive is not in a ready state.

**Recommended Action:** This error may occur when a request for non-robotic media had caused a pending request in the device monitor, and the operator has assigned the request to a drive that is not in a ready state. This error is not a fatal error. The request will pend again in the NetBackup device monitor. Verify that required tape is in the drive it is assigned to, and that the drive ready light has come on. It may take some time for the drive to become ready after the tape has been



inserted. If the drive never goes to a ready state after a tape has been inserted, there may be a problem with the drive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2038

**Message:** Media loaded in drive is not write-enabled

**Explanation:** This error may occur when a storage unit request for non-robotic media had caused a pending request in the device monitor, and the operator has inserted media that is not write enabled into the drive.

**Recommended Action:** This is not a fatal error. The request will pend again in the NetBackup device monitor. If you are sure that it is OK to write on this tape, verify that the required tape has its write enable switch set to allow write.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2039

**Message:** SCSI reservation conflict detected

**Explanation:** The NetBackup `bptm` component was unable to read or write a tape drive because another job unexpectedly holds a SCSI reservation for the drive.

**Recommended Action:** This error should never occur at job resource allocation time, but may occur during i/o for a tape job. The verbose `bptm` logs on the media server may be useful in understanding the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2040

**Message:** Maximum job count has been reached for the storage unit

**Explanation:** Storage cannot be allocated because it would exceed maximum job count. The maximum job count is configurable for each storage unit. Multiple copy jobs may cause this same error, if there are more copies targeted for a storage unit than the amount of copies for which the storage unit was configured.

**Recommended Action:** Target a different storage unit with one of the copies, or increase the maximum job count for the storage unit.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2041

**Message:** Storage unit is down

**Explanation:** A disk storage unit has been designated as down and cannot be used.

**Recommended Action:** Run the `bpererror -disk` command to indicate why the disk is considered down.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2042

**Message:** Density mismatch detected

**Explanation:** This error is an internal NetBackup error. A job has requested media with the wrong density. A mismatch may exist between the image catalog and the media database.

**Recommended Action:** Restore the jobs request tape media by media ID density. If the requested density does not match the configured density for the media, it cannot be allocated.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2043

**Message:** Requested slot is empty

**Explanation:** Media is not found in the expected slot in the robot.

**Recommended Action:** The robot may need to be inventoried.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2044

**Message:** Media is assigned to another application

**Explanation:** Requested media cannot be allocated because it is assigned to an application other than NetBackup.

**Recommended Action:** Verify that the media that is required for the job is assigned to NetBackup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2045

**Message:** Storage unit is disabled since max job count is less than 1

**Explanation:** Storage unit cannot be used because its maximum job count is set to 0.

**Recommended Action:** Increase the maximum job count (or maximum concurrent drive count) to a value greater than 0.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2046

**Message:** Media is unmountable

**Explanation:** Media has been marked as unusable due to mount errors.

**Recommended Action:** Clean the drives in the media's robot. Determine if any of the media is bad.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2047

**Message:** Media is write protected

**Explanation:** The media cannot be used for a write job because it is write protected.

**Recommended Action:** Make sure that media in the scratch pool is not write protected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2048

**Message:** Media is in use by the ACS robotic library

**Explanation:** ACS media that is required by this job is in use on another system.

**Recommended Action:** Make sure that the required media is not in use by another application.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2049

**Message:** Media not found in the ACS robotic library

**Explanation:** Media that this job needs is not found in the ACS robotic library.

**Recommended Action:** Make sure that the required media is available in the ACS robot.

For more information, see the section on configuring ACSLS robots in the [NetBackup Device Configuration Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2050

**Message:** ACS media has an unreadable external label

**Explanation:** This job needs the ACS media that cannot be used because its external label or barcode is unreadable.

**Recommended Action:** Correct the barcode label problem for this media.

For more information, see the section on configuring ACSLS robots in the [NetBackup Device Configuration Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2051

**Message:** ACS media is not in the drive's domain

**Explanation:** Media that is required for this job is in an ACS robot that is not accessible.

**Recommended Action:** Verify that the robot that contains the required media is accessible to a NetBackup media server.

For more information, refer to the section on configuring ACSLS robots in the [NetBackup Device Configuration Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2052

**Message:** An ACS Library Storage Module (LSM) is offline

**Explanation:** The required ACS LSM is offline.

**Recommended Action:** Bring the ACS LSM online.

For more information, see the section on configuring ACSLS robots in the [NetBackup Device Configuration Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2053

**Message:** Media is in an inaccessible drive

**Explanation:** The required media is currently loaded in a DOWN or otherwise inaccessible drive.

**Recommended Action:** Locate the media and correct the problem that has caused the drive or drive path to be down.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2054

**Message:** Media is in a drive that is currently in a DOWN state

**Explanation:** Required media is currently loaded in a drive that is down.

**Recommended Action:** Locate the media and correct the problem that has caused the drive or drive path to be down.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2055

**Message:** ACS physical drive is not available

**Explanation:** The media server cannot load ACS media because a drive is not available.

**Recommended Action:** Locate and install an ACS drive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2056

**Message:** The file name used for the mount request already exists

**Explanation:** The `tpreq` command cannot load this media because the specified file name already exists.

**Recommended Action:** Specify a different file name for `tpreq`, or run the `tpunmount` command for the media which has been loaded using `tpreq` with the conflicting file name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2057

**Message:** The scan host of the drive is not active

**Explanation:** The scan host for a standalone drive is offline, so the drive cannot be allocated.

**Recommended Action:** If the problem persists, restart the NetBackup media servers that have paths to this drive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2058

**Message:** LTID needs to be restarted on media servers before the device can be used

**Explanation:** A drive cannot be used because an `ltid` restart is required. This error may occur when configuration changes have been made on a media server, but `ltid` has not been subsequently restarted.

**Recommended Action:** When the media server is not in a busy state, stop and restart `ltid` on that media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2059

**Message:** The robotic library is not available

**Explanation:** The robot that is required for a drive cannot be found in the `nbemm` database.

**Recommended Action:** Verify that the robot that the jobs require is properly configured. If the error persists, the following logs may be useful in understanding the problem: The `mds` unified logging files (OID 143) from the master server at debug level 2.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2060

**Message:** Media needs to be rewound or unmounted from a drive

**Explanation:** The NetBackup `mds` component uses this error internally to inform the Resource Broker that a tape needs to be unloaded. It should never appear as a job error status.

**Recommended Action:** Not applicable.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2061

**Message:** The host is not an active node of a cluster

**Explanation:** A cluster failover has occurred while a job is running. A job may be waiting for a span on a media server that has failed over.

**Recommended Action:** Restart the failed job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2062

**Message:** Throttled job count has been reached for the storage unit

**Explanation:** This error is not returned as a job status.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2063

**Message:** Server is not licensed for the Remote Client Option

**Explanation:** The media server required for this job does not have the Remote Client Option enabled. A SAN media server is asked to back up a client that is not also a media server, or a VMware backup is tried on a SAN media server.

**Recommended Action:** Backup this client on a media server that is licensed to do so. Verify that the media server has connectivity to the master server when adding its licenses.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2064

**Message:** Job history indicates that no media is available

**Explanation:** When a job is run on a media server that is installed with invalid NetBackup software, there are some situations where the job starts, but media is not available for the job. In this case, the master server stops using that storage unit for a period of time (12 hours), and returns this error for jobs requested the storage unit.

**Recommended Action:** Make sure that media is available for the storage unit. If necessary, upgrade the software on the media server. Add media if necessary. If media is available, wait 12 hours until the storage unit can be used again. To make the storage unit immediately usable, run the following command on the master server to release the hold:

```
nbrbutil -releaseAllocHolds
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2065

**Message:** Job history indicates that no drive is available

**Explanation:** When a job is run on a media server that is installed with invalid NetBackup software, there are some situations where the job starts, but the drives that are designated for the job are busy or otherwise unavailable, causing the job to fail. In this case, the NetBackup master server stops using that drive for a period of time (several minutes), and returns this error for jobs requesting that drive.

**Recommended Action:** Upgrade the media server software. Make sure all of the drives in the storage unit are up and available for use. Clean all drives that need cleaning.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2066

**Message:** Disk pool not found



**Explanation:** A job has been targeted for a disk pool that does not exist in the `nbemm` database.

**Recommended Action:** Verify that the storage unit that this job uses is configured for use with a properly configured disk pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2067

**Message:** Disk volume not found

**Explanation:** A read job requires a disk volume that does not exist in the `nbemm` database. Or a write job is configured for a disk pool with no configured volumes.

**Recommended Action:** Verify that the disk storage that this job uses is configured for use with a disk pool that has volumes configured. For a read job, verify that the volume that is required for reading exists in the `nbemm` database.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2068

**Message:** Disk volume mount point not found

**Explanation:** A disk volume is not configured with a mount point or not completely configured in the `nbemm` database.

**Recommended Action:** Verify that the configuration is correct for the disk group and for the disk volumes in the disk group.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2069

**Message:** Disk volume mount point record insert failed

**Explanation:** A database update has failed while trying to allocate a disk job.

**Recommended Action:** This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.

- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2070

**Message:** The specified mount path will not fit in the allocated space

**Explanation:** A disk volume mount point path is larger than the allowed maximum.

**Recommended Action:** This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2071

**Message:** Unable to find any storage servers for the request

**Explanation:** NetBackup was unable to find a storage server for this disk job.

**Recommended Action:** Verify that the storage servers serving the disk group that the job requires are configured and enabled. Verify that they are in an UP state.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2072

**Message:** Invalid operation on static mount point

**Explanation:** An incorrectly configured mount point has been found for a disk volume.

**Recommended Action:** This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.

- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2073

**Message:** Disk pool is down

**Explanation:** Required disk pool cannot be used because it is in a DOWN state.

**Recommended Action:** Run the `bperorr -disk` command to determine why the disk pool was put into a DOWN state. Correct the problem, and use the `nbdevconfig` command to return the disk pool to an UP state.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2074

**Message:** Disk volume is down

**Explanation:** Required disk volume cannot be used because it is in a DOWN state.

**Recommended Action:** You may be able to see why the disk volume was put into a DOWN state by running `bperorr -disk`. Correct the problem, and use `nbdevconfig` to return the disk volume to an UP state.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2075

**Message:** Fibre Transport resources are not available

**Explanation:** A job is configured to require Fibre Transport for this SAN client, but no available Fibre Transport connection exists.

**Recommended Action:** Configure the job to switch to LAN transport if Fibre Transport is not available. Verify that the job type being run is compatible with Fibre Transport. Using `nbdevquery`, verify that the Disk Pool being requested is enabled for use with Fibre Transport. Verify that there are Fibre Transport connections that are up between the client and media server required for the job. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.

- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2076

**Message:** DSM returned an unexpected error

**Explanation:** The Disk Service Manager component of NetBackup has returned an unexpected error.

**Recommended Action:** This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2078

**Message:** The maximum number of mounts for the disk volume have been exceeded

**Explanation:** A disk volume cannot be used by a job because it is mounted by too many other users.

**Recommended Action:** This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2079

**Message:** DSM has detected that an invalid file system is mounted on the volume

**Explanation:** NetBackup did not find the file system it expected on a disk volume.

**Recommended Action:** Verify that the disk volumes and their associated mount points that NetBackup uses are not used by other applications.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2080

**Message:** Disk volume has no max writers count

**Explanation:** Disk volume is not properly configured for a usable number of mountpoints.

**Recommended Action:** Verify proper disk configuration by using `nbdevquery`. This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2081

**Message:** Disk volume has no max readers count

**Explanation:** Disk volume is not properly configured for a usable number of mountpoints.

**Recommended Action:** Verify the proper disk configuration by using `nbdevquery`. This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2082

**Message:** The drive needs to be marked as available

**Explanation:** Drive cannot be used because it is allocated with loaded media, but MDS has not made it available for use.

**Recommended Action:** Run the `nbrbutil -dump` command on the master server to show allocations for this job. If the problem persists, run the `nbrbutil -releaseMDS` command to release the allocation for the drive so it can be used.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2083

**Message:** The media affinity group is not defined in EMM

**Explanation:** MDS expected to find a group of reservations for this media, but did not find the expected reservation group.

**Recommended Action:** This error is internal. If the problem persists, check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2084

**Message:** Media affinity group record insert failed

**Explanation:** MDS cannot update reservation group information for this tape media.

**Recommended Action:** This error is internal. If the problem persists, check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2085

**Message:** Disk volume is not available

**Explanation:** The job requires more disk volumes than are currently configured.

**Recommended Action:** Ensure that the disk group has disk volumes configured. A multiple copy job cannot target two copies for the same disk volume.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2086

**Message:** Disk volume cannot be used for more than one copy in the same job

**Explanation:** Not enough eligible disk volumes are configured for this multiple copy job.

**Recommended Action:** Use the `nbdevquery -listdv` command to verify that the expected disk volume is configured. For a multiple copy job, ensure that unique eligible disk volumes exist for each copy. A multiple copy job cannot target two copies for the same disk volume.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2087

**Message:** Media allocation would exceed maximum partially full media limit

**Explanation:** You cannot run this job because it would exceed configured limit of maximum partially full media.

**Recommended Action:** This error may occur with a multiple copy job or a duplication job. If the problem persists, you may need to increase maximum partially full media setting on the disk pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2088

**Message:** Cleaning media is not available

**Explanation:** You cannot run a cleaning job because no cleaning media is configured for the drive.

**Recommended Action:** Add a cleaning volume to the robot containing the drive.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2089

**Message:** FT client is not running

**Explanation:** This job requires Fibre Transport, but the Fibre Transport client is not running on the client that is required for this job.

**Recommended Action:** Do one or more of the following:

- Verify that the Private Branch Exchange (PBX) service is installed and running. Run the `bpps -x` command to ensure that `pbx_exchange` is listed in the processes that are running.
- Verify that the client is configured as a SAN Client. Run the `bpcIntcmd -sanclient` command to return the current state of the SAN Client. A response of 0 (zero) indicates that SAN Client is not configured. Rerun the command as `bpcIntcmd -sanclient 1`.
- Verify that the client is not also a media server, master server, or EMM server. The SAN Client process runs only on a NetBackup client.
- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server.
- Verify that no server entries for the SAN Client exist on the NetBackup master server. Remove any `SERVER=clientname` entry in the master server for the SAN Client. If the master server has the SAN Client listed also as a server, it may shutdown the SAN Client.
- Restart the SAN Client service. The SAN Client restarts when the server reboots, but does not automatically restart after you run the `bpcIntcmd` command. To start the SAN Client service, run the client startup script or use the Service Manager in Windows.

For more information, see the Troubleshooting chapter of the [NetBackup SAN Client and Fibre Transport Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2090

**Message:** FT client has no devices configured



**Explanation:** This job requires Fibre Transport, but Fibre Transport devices are not configured on the client that is required for this job.

**Recommended Action:** Verify that Fibre Transport devices are installed on the client. For further information, see the Troubleshooting chapter of the *NetBackup SAN Client and Fibre Transport Guide* available at the following location:

<http://www.veritas.com/docs/DOC5332>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2091

**Message:** FT client devices are offline

**Explanation:** This job requires Fibre Transport, but all Fibre Transport devices are offline on the client that is required for this job.

**Recommended Action:** Do one or more of the following:

- Verify that the Private Branch Exchange (PBX) service is installed and running. Run the `bpps -x` command to ensure that `pbx_exchange` is listed in the processes that are running.
- Verify that the client is configured as a SAN Client. Run the `bpcintcmd -sanclient` command to return the current state of the SAN Client. A response of 0 (zero) indicates that SAN Client is not configured. Rerun the command as `bpcintcmd -sanclient 1`.
- Verify that the client is not also a media server, master server, or EMM server. The SAN Client process runs only on a NetBackup client.
- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server.
- Verify that no server entries for the SAN Client exist on the NetBackup master server. Remove any `SERVER=clientname` entry in the master server for the SAN Client. If the master server has the SAN Client also listed as a server, it may shutdown the SAN Client.
- Restart the SAN Client service. The SAN Client restarts when the server restarts, but does not automatically restart after you run the `bpcintcmd` command. To start the SAN Client service, run the client startup script or use the Service Manager in Windows.

For further information, see the Troubleshooting chapter of the [NetBackup SAN Client and Fibre Transport Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2092

**Message:** FT server devices for client are offline

**Explanation:** This job requires Fibre Transport, but all Fibre Transport devices are offline on the media server required for this job.

**Recommended Action:** Do one of the following:

- Verify that marked QLogic Target ports exist in the server. The `nbftsrvr` and `nbfdrv64` processes exit if the system has no ports available for Target Mode use.
- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature that requires a key called "SAN Client" on the master server. The Fibre Transport server performs a license check during startup.
- Determine if a reboot is required for the installation of the Fibre Transport server. Solaris installations require that you reboot the media server after you install Fibre Transport to load the Fibre Transport drivers on the marked target ports. In addition, reboot the Linux servers if you choose to not unload the existing QLogic drivers during the installation of Fibre Transport.

For further information, see the Troubleshooting chapter of the [NetBackup SAN Client and Fibre Transport Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2093

**Message:** No FT servers for this client are running

**Explanation:** This job requires Fibre Transport, but no Fibre Transport devices are configured with connectivity to the media server that is required for this job.

**Recommended Action:** Do one of the following:

- Verify that marked QLogic Target ports exist in the server. The `nbftsrvr` and `nbfdrv64` processes exit if the system has no ports available for Target Mode use.
- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN

Client" on the master server. The Fibre Transport server performs a license check during startup.

- Determine if a reboot is required for the installation of the Fibre Transport server. Solaris installations require that you reboot the media server after you install Fibre Transport to load the Fibre Transport drivers on the marked target ports. In addition, reboot the Linux servers if you choose to not unload the existing QLogic drivers during the installation of Fibre Transport.

For further information, see the [NetBackup SAN Client and Fibre Transport Troubleshooting Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2094

**Message:** STU cannot run Lifecycle backups

**Explanation:** The storage lifecycle job cannot run because the targeted disk pool is not enabled for Storage Lifecycles.

**Recommended Action:** Run the `nbdevquery -listdp` command to check the configuration of the disk pool. If the Lifecycle attribute is not enabled for the disk pool, run the `nbdevconfig -changedp -setattribute` command to enable it.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2095

**Message:** STU cannot run VMware backup

**Explanation:** The media server that is configured for this job's storage unit cannot run VMware backups.

**Recommended Action:** To run a VMware backup, the media server must run a valid version of NetBackup. Verify that a valid version of NetBackup is running or configure the backup for a media server that runs a valid version of NetBackup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2096

**Message:** NDMP operation does not support multiple inline copies

**Explanation:** The backup cannot run because it is an NDMP policy and is configured for multiple copies.

**Recommended Action:** NetBackup cannot make multiple copies of NDMP policies. Configure the backup for a single storage unit destination.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2097

**Message:** Storage unit group does not exist in EMM configuration

**Explanation:** You cannot run this job because it is configured to use a storage unit group that does not exist in the NetBackup configuration.

**Recommended Action:** Reconfigure the policy to use a storage unit or storage unit group that exists in the configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2098

**Message:** Media pool is not eligible for this job

**Explanation:** This job is configured to use a pool that does not exist in the NetBackup configuration.

**Recommended Action:** Change the configured media pool for the job to use a pool that is configured, or create the required media pool. Make sure that the media pool you have configured for the job is not a scratch pool.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2099

**Message:** Required drive or drive path is not configured

**Explanation:** This job requires a drive that does not exist in the NetBackup configuration.

**Recommended Action:** Run the `vmopr cmd` command to verify the drive configuration. Configure the drives that are necessary for the media type that is used.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2100

**Message:** Maximum number of mounts has been exceeded for tape media

**Explanation:** The job cannot run because the required media has exceeded configured maximum mounts.

**Recommended Action:** Increase the maximum allowed mounts for the media. You may need to retire this media if it has exceeded the maximum number of mounts you have configured.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2101

**Message:** Media server not found in EMM database

**Explanation:** The possible causes include the following:

- For a tape backup, the media server that performed the backup is not in the EMM database.
- For an OpenStorage optimized duplication job, the media server in common between the source environment and the target environment does not have the credentials for both storage servers.

**Recommended Action:** Do the following as appropriate:

- For a restore from tape, you can use the Force Media Server Restore option to force NetBackup to replace the missing media server with a new media server.
- For optimized duplication, ensure that the media server in common has credentials for both storage servers. More information about OpenStorage optimized duplication is available.

See the [NetBackup OpenStorage Solutions Guide for Disk](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2102

**Message:** Storage unit does not support spanning

**Explanation:** A disk job has requested a span for a disk type that does not support spanning.

**Recommended Action:** Some disk types do not support spanning. Run the `nbdevconfig -listdg` command to determine if a disk group supports spanning.

If this error persists, ensure that enough space is available on your disk storage units for the new jobs that are running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2103

**Message:** Media server mismatch

**Explanation:** This error may occur when a multiple copy job is configured for the storage units that have no common media server.

**Recommended Action:** All copies of a multiple copy job must run on the same media server. Configure the storage units that have drive paths or disk access from a common media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2104

**Message:** Storage units are not available

**Explanation:** This error may occur for multiple copy jobs that are configured so that no possible storage unit combination can be used.

**Recommended Action:** Verify that all criteria in met for the policy with the storage units that are configured.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2105

**Message:** Storage unit requested for replication job is not replication capable

**Explanation:** This error can occur when a replication job requests a storage unit for write, but the disk that the storage unit calls out is not replication enabled.

**Recommended Action:** Make sure that replication jobs include status configured for replication enabled disks in their storage unit specifiers.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2106

**Message:** Disk storage server is down

**Explanation:** This error can occur when a job uses a disk storage unit whose disk group resides on a storage server that NetBackup has marked down. This error can also occur when a cloud storage backup fails.

**Recommended Action:** Verify that all media servers that are configured for the storage server can communicate with the storage server. The `bpstsinfo` command queries the storage server periodically, so you can use the `bpstsinfo` log set to verbosity level 5 on the media server.

If the error is related to a cloud storage backup failure, you should verify the following information:

- The NetBackup CloudStore Service is running on the master and media servers. See the *NetBackup CloudStore Service Container startup and shutdown troubleshooting* section in the *NetBackup Cloud Administrator's Guide* for information on how to start the service. This guide is available at the following location:  
<http://www.veritas.com/docs/DOC5332>
- The NetBackup certificates are stale/unavailable on the configured media server, which can cause the storage server to go down. Ensure that you deploy all of the required certificates on that media server to keep the storage server up. For more information, see the *NetBackup Security Encryption Guide* at the following location:  
<http://www.veritas.com/docs/DOC5332>
- The **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server is selected if the media server is version 8.0 or earlier. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2107

**Message:** Requested media server does not have credentials or is not configured for the storage server

**Explanation:** A job has requested disk media for a media server that does not have credentials to access the disk storage server. During optimized duplication between two storage servers of the same type, a media server that is configured for the write side storage unit may not have credentials to access the read side storage server.

**Recommended Action:** Optimized duplication requires a media server with credentials for both the read side and write side storage servers. Add the needed credentials or limit the media servers that the write side storage unit calls out to those that are credentialed for the read media.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2108

**Message:** Requested NDMP machine does not have credentials or is not configured in NetBackup

**Explanation:** A job requests the use of an NDMP machine that is not configured in NetBackup.

**Recommended Action:** Jobs for NDMP policies require that the NDMP host that is specified as the client in the policy be configured in NetBackup. The credentials that are defined for any server must access the NDMP host.

Verify that the required NDMP host is configured. If the configured NDMP host is a fully qualified name and the NDMP host name in the policy is not, run the following command to add an alias to the NDMP host:

```
# nbemmcmd -machinealias -addalias -alias string -machinename string
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2109

**Message:** Requested Fibre Transport client machine was not found in NetBackup configuration

**Explanation:** A job requests a Fibre Transport client machine that is not found in the NetBackup configuration.

**Recommended Action:** Fibre Transport backup and restore operations require each Fibre Transport client to be configured in NetBackup. Verify that the client that is requested for the job is configured as a Fibre Transport client.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2110

**Message:** Requested machine is not configured in NetBackup



**Explanation:** A job has requested a machine that is not configured in NetBackup.

**Recommended Action:** The policy that you use to run the job may indicate which server the job requires. If not, find the server that the job looks for by setting the MDS VxUL logging (OID 143) to debug level 2 and retry the job. The MDS log usually indicates which host name caused the problem.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2111

**Message:** All storage units are configured with On Demand Only and are not eligible for jobs requesting ANY storage unit

**Explanation:** A job has requested any available storage unit, but all storage units are configured with On Demand Only.

**Recommended Action:** Change the policy to use a specific storage unit instead of any available storage unit, or configure at least one storage unit without the On Demand Only setting.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2112

**Message:** NetBackup media server version is too low for the operation

**Explanation:** The storage unit or storage unit group points to a media server that runs an earlier version of software than the master server. Hence, the media server cannot use all the functionality of the newer NetBackup version. This mismatch of software affects many write operations such as backup operations and duplication write operations.

**Recommended Action:** Point the storage unit to a media server with a newer version of software.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2113

**Message:** Invalid or no disk array credentials are added for vserver

**Explanation:** Invalid or no credentials found in Disk Array Hosts credential section for NetApp Storage Virtual Machine's interface name having management access enabled.

**Recommended Action:** Under the Disk Array Hosts credentials section, add admin credentials of NetApp Storage Virtual Machine's interface that has management access enabled. Ensure that the right Storage Virtual Machine's interface name is entered that holds the snapshot/replica to be indexed. Ensure that the Storage Virtual Machine (SVM) user account with the ONTAP application is in the unlocked state.

See the [NetBackup Replication Director Solutions Guide](#) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2504

**Message:** Direct expiration of a mirror copy is not allowed

**Explanation:** The mirror copy alone cannot be expired. It expires when the parent copy expires.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2517

**Message:** Backup set identifier may only contain a-z, A-Z, 0-9 and .-+ \_

**Explanation:** An Oracle backup set identifier (TAG) contains an invalid character outside of the following characters: a-z, A-Z, 0-9 and special characters ., -, +, and \_.

**Recommended Action:** Remove the invalid character from the backup set identifier. This value is specified in the **Attributes** tab of the GUI **Policy** utility.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2521

**Message:** Datafile copy tag may only contain a-z, A-Z, 0-9 and .-+ \_

**Explanation:** The Datafile copy tag contains an invalid character outside of the following characters: a-z, A-Z, 0-9 and special characters ., -, +, and \_.

**Recommended Action:** Remove the invalid character from the Datafile copy tag. This value is specified in the **Oracle** tab of the GUI **Policy** utility.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2522

**Message:** Oracle policy cannot include a pluggable database with a FRA backup.

**Explanation:** NetBackup does not support FRA with Oracle 12c pluggable databases.

**Recommended Action:** Check the Oracle Intelligent Policy. If the policy has **Protect Instances and Databases** selected and includes pluggable databases, then the backup selection cannot be **Fast Recovery Area (FRA)**. You can either select a different backup selection or select the Oracle 12c instance and **Fast Recovery Area (FRA)**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2523

**Message:** Failed to add client to NetBackup configuration.

**Explanation:** There was an internal error when a client was added to the configuration. This type of error can occur after the domain name is changed.

**Recommended Action:** Save the `nbemm` and `bpdbm` logs and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2524

**Message:** Catalog backup failed because the passphrase for the disaster recovery package is not set.

**Explanation:** During the catalog backup, the disaster recovery package is created. NetBackup requires the passphrase when it creates the disaster recovery package. If the passphrase has not already been set, the catalog backup fails.

**Recommended Action:** To set the passphrase for the disaster recovery package, do one of the following:

- In the **NetBackup Administration Console**, expand **Security Management** > **Global Security Settings**. On the **Disaster Recovery** tab, set the passphrase.
- Use the `nbseccmd -drpkgpassphrase` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2525

**Message:** The passphrase for the disaster recovery package is not set. You must set it for the catalog backups to be successful.

**Explanation:** During the catalog backup, the disaster recovery package is created. NetBackup requires the passphrase when it creates the disaster recovery package. If the passphrase is not set earlier, the catalog backup fails.

The error message is displayed when you configure the catalog backup policy. You should set the passphrase before you configure the catalog backup policy.

**Recommended Action:** To set the passphrase for the disaster recovery package, do one of the following:

- In the **NetBackup Administration Console**, expand **Security Management** > **Global Security Settings**. On the **Disaster Recovery** tab, set the passphrase.
- Use the `nbseccmd -drpkgpassphrase` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2800

**Message:** Standard policy restore error

**Explanation:** Some or all of the restore operation files failed. When performing a Snapshot Client restore, you may have selected a different path from the path in the policy's **Backup Selections** list.

For example, `vol6` is mounted on `/mnt/vol6` and `vol7` is mounted on `/mnt/vol7`. These mount points are specified in the backup selection. If you select only the parent directory (`/mnt`), the restore fails with status code 2800.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages about why the restore failed. Also, check the All Log Entries report on the server.
- Check the following logs for additional failure information:
  - NetBackup `tar` log
  - Master server: `bprd`, `nbjm`

- **Media server:** `bpbrm`, `bptm`, `bpdm`
- **Client:** `tar`
- Make sure that the required media server is available for the restore, or use the **Media host override** option.
- Verify that the media that is required for the restore is present and that the robot has been inventoried.
- Verify that no network issues exist between the media server and the client.
- Select the original path that is listed in the **Backup Selections** tab.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2801

**Message:** Oracle policy restore error

**Explanation:** An error caused the restore of the Oracle data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check ownership and permission on the Oracle instance that you restore.
- Check the NetBackup `dbclient` and `user_ops` logs for additional failure information.
- If restoring to an alternate client using RMAN, more information is available in the following technical article:  
<http://www.veritas.com/docs/TECH5840>  
 Check that the Oracle user on the client can successfully communicate with the master server by using the `bpclntcmd -pn` command.
- Check that the Oracle user on the client can see the backup images on the master by using the `bplist` command.
- On UNIX and Linux hosts, check that the oracle user has sufficient permissions to read `/etc/services`, `/etc/nsswitch.conf`, and `/usr/openv/netbackup/bp.conf`.

- Ensure that the Oracle database is linked correctly, according to the [NetBackup for Oracle Administrator's Guide](#) (for example, `$ORACLE_HOME/lib/libobk.so`). More information is available in the following technical article:  
<http://www.veritas.com/docs/TECH72307>
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2802

**Message:** Informix-On-BAR policy restore error

**Explanation:** An error caused the restore of the Informix data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check ownership and permission on the Informix instance that you restore.
- Check the NetBackup `infxbsa` and `user_ops` logs from the client, and the `bprd` log from the master server for additional failure information.
- Check the Informix `BAR_ACT_LOG`, `BAR_DEBUG_LOG`, and `MSGPATH` logs for additional failure information.
- For large database restores, you may need to increase the client read timeout value.
- If you are restoring to an alternate client, review the checklist in the following article:  
<http://www.veritas.com/docs/TECH21719>
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2803

**Message:** Sybase policy restore error

**Explanation:** An error caused the restore of the Sybase data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on the Sybase instance that you restore and on the directories where files are restored.
- Check the NetBackup `sybackup` log for additional failure information.
- Create the following log folders, then retry the restore:  
On the client:

```
/usr/opensv/netbackup/logs/bphdb
/usr/opensv/netbackup/logs/bprestore
/usr/opensv/netbackup/logs/tar
/usr/opensv/netbackup/logs/sybackup
chmod 777 /usr/opensv/netbackup/logs/sybackup
chmod 777 /usr/opensv/netbackup/logs/bphdb
```

On the media server:

```
/usr/opensv/netbackup/logs/bptm
/usr/opensv/netbackup/logs/bpbrm
```

On the master server:

```
/usr/opensv/netbackup/logs/bprd
```

- Correct the problems that you find and retry the restore.

To set the debug level on UNIX and Linux clients, enter the following line in the `bp.conf` file:

```
VERBOSE = 5
```

For a Sybase alternate client restore, the user ID (UID) of the restoring Sybase backup server must match the UID of the Sybase backup server from the source host.

For an alternate client restore, authorize the alternate client to access images for the original client.

Verify that the alternate client can browse the backup images for the original client:

```
# /usr/opensv/netbackup/bin/bplist -C <origClient> -t 7 -l -R /
# install_path\netbackup\bin\bplist -t 7 -l -R /
```

On the alternate client, use the `bpcIntcmd` command to test connectivity and name resolution. The command should display the name of the master server on the first line. The second line must contain the IP address of the network interface that the alternate client used when communicating with the master server. The first word on the second line is the name of the alternate client as resolved on the master server from the IP address. The second word on the second line may be 'NULL' if the alternate client is not being backed up. Otherwise, it is the name of the alternate client (or an alias) which is defined in a backup policy on the master server.

```
# /usr/openv/netbackup/bin/bpcIntcmd -pn
```

Make sure that `CLIENT_READ_TIMEOUT` on the alternate client and media server is set large enough to allow the tapes to be read, the data transferred, and the database instance to write the data to disk.

See the following technical article for information about the steps for a Sybase alternative client restore operation:

<http://www.veritas.com/docs/TECH24125>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2804

**Message:** MS-SharePoint policy restore error

**Explanation:** An error caused the restore of the SharePoint data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Create the following log folders on the SQL Server, the front-end web server, the media server, and the master server:

```
install_path\NetBackup\logs\tar
install_path\NetBackup\logs\bpresolver
install_path\NetBackup\logs\bpbrm (media server)
install_path\NetBackup\logs\bprrd (master server)
```

If you use granular restore technology (GRT), the following log folders also apply:



```
install_path\NetBackup\logs\ncf
install_path\NetBackup\logs\ncflbc
install_path\NetBackup\logs\ncfgre
install_path\NetBackup\logs\nbfsc
install_path\NetBackup\logs\spsv2ra
```

- Check all SharePoint server Event Viewers (application and system) for any errors.
- Connect to the server where the SharePoint front-end server runs and launch the restore using Backup, Archive, and Restore GUI.
- Make sure that the restore is being launched correctly.  
See the [NetBackup for Microsoft SharePoint Administrator's Guide](#).
- Correct the problems that you find and retry the restore.
- If you need to restore a VMware job, you must ensure that the media server is added to the additional server list. To access this list in the **NetBackup Administration Console**, expand **Host Properties > Master Server**. Double-click the name of the server to view the properties. Select the **Servers** tab to display the server list. In the **Servers** properties dialog box, select the **Additional Servers** tab and add the media server to the server list.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2805

**Message:** MS-Windows policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check that you have selected the correct restore type on the Backup, Archive, and Restore GUI.
- Check ownership and permission on directories where files are restored.
- Check the following logs for additional failure information:
  - Master server: bprd, nbjm
  - Media server: bpbrm, bptm, bpdm

- Client: `tar`
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2806

**Message:** NetWare policy restore error

**Explanation:** An error caused the restore of the NetWare data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup `tar` log for additional failure information. Also check the following log files: `bpcd`, `bpsrv`, `bprest`, and `user_ops`.
- For target restores, ensure that you have create and write rights to the volume that you are trying to restore. In the `BP.INI` file, ensure that the `Allow_Server_Write` parameter is set to yes.
- If you launched a non-target restore from the **NetBackup Administration Console**, ensure that the **Allow server directed restores** parameter is selected.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2807

**Message:** SQL-BackTrack policy restore error

**Explanation:** An error caused the restore of the SQL-BackTrack data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.

- Check ownership and permission on directories where files are restored and on the SQL-BackTrack instance that you are restoring.
- Check the NetBackup backtrack log for additional failure information.
- Ensure that the `No.Restrictions` file has been added on the master server in case of an alternate client restore.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2808

**Message:** Windows File System policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check that you have selected the correct restore type on the Backup, Archive, and Restore GUI.
- Check ownership and permission on directories where files are restored.
- Check that the destination directories or files exist. If so, select the **Overwrite existing files** option on the **Backup, Archive, and Restore** GUI.
- Check the following logs for additional failure information:
  - Master server: `bprd`, `nbjm`
  - Media server: `bpbrm`, `bptm`, `bpdm`
  - Client: `tar`
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2809

**Message:** MS-SQL-Server policy restore error

**Explanation:** An error caused the restore of the SQL Server data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored and on the SQL instance that you are restoring.
- Check ownership and permission on the SQL Server instance and on the directories where files are restored.
- Check the following logs for additional failure information on the client side:

```
install_path\NetBackup\logs\dbclient
install_path\NetBackup\logs\bpbkar (Snapshot Client)
install_path\NetBackup\logs\bpfis (Snapshot Client)
install_path\NetBackup\logs\bppfi (instant recovery)
```

- Check the SQL server Event Viewers (application and system) for any errors or messages that are related to the restore operation.
- Increase restore verbose levels.  
See the [NetBackup for SQL Server Administrator's Guide](#).  
Review this guide to verify that you launched the restore correctly.
- Connect to the server where SQL is running and launch the restore from that server using the Backup, Archive, and Restore GUI.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2810

**Message:** MS-Exchange policy restore error

**Explanation:** An error caused the restore of the Exchange data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.

- Check ownership and permission of the Exchange instance that you restore and the directories where files are restored.
- Verify the following log files depending on the type of restore being performed. All the log folders are located in the `install_path\NetBackup\logs` folder.

- `beds` - All restore operations.
- `tar` - All restore operations.

Restores with Granular Recovery Technology (GRT):

- `nbfsd` - This log appears on the client and the media server.
- `ncf` - This log uses unified logging and appears on the destination client or proxy client.
- `ncflbc` - This log is for `nblbc.exe`. It appears on the destination client or proxy client.
- `ncfgre` - This log is for `nbgre.exe`. It appears on the destination client or proxy client.

Instant Recovery and Instant Recovery off-host:

- `bpbkar` - For off-host Instant Recovery restores, `bpbkar` logs on the alternate client.
- `bpfis` - This log applies to Instant Recovery rollback restores. For off-host Instant Recovery backups, `bpfis` logs exist on both the primary and the alternate clients.
- `bppfi` - For off-host Instant Recovery restores, `bppfi` logs on both the primary and the alternate clients.
- Check the Exchange Server Event Viewer for Application and System messages that are related to the restore operation.
- Connect to the server where Exchange is running and launch the restore from that server using the Backup, Archive, and Restore GUI.
- Verify that you launched the restore correctly.  
See the [NetBackup for Microsoft Exchange Server Administrator's Guide](#).
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2811

**Message:** SAP policy restore error

**Explanation:** An error caused the restore of the SAP data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission of the SAP instance that you restore and the directories where the files are restored.
- Ensure that the `No.Restrictions` file has been created on the master server in case of an alternate client restore.
- Check the following logs for additional failure information: `backint`, `tar`, `dbclient`, `bprestore`, and `user_ops`.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2812

**Message:** DB2 policy restore error

**Explanation:** An error caused the restore of the DB2 data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission of the DB2 instance that you restore and the directories where the files are restored.
- Check the NetBackup `bpdb2` log for additional failure information.
- Ensure that you configured the clients to allow redirected restores. See the [NetBackup for DB2 Administrator's Guide](#) for details.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2813

**Message:** NDMP policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check the ownership and permission on directories where files are restored.
- Verify that the destination NDMP host supports DAR. If not, disable DAR.
- Check the `ndmpagent` (Originator ID 134) log for additional failure information.
- Check the NetBackup `bptm` log for additional failure information.
- Check that the **Force rollback even if it destroy snapshots** option of the point-in-time rollback restore is set (checked) or not set (unchecked).  
 For more information on rollback restore, please see the *NetBackup Replication Director Solutions Guide* from the following location:  
<http://www.veritas.com/docs/DOC5332>
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2814

**Message:** FlashBackup policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup `tar` log for additional failure information.
- Enable and verify VxMS logs for additional failure information.
- For VMware restores, enable the `bpyvmutil` logs.

- If you run a VMware restore, make sure that the user account that is specified in the VMware credentials has full administration rights on the target vCenter and the ESX server.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2815

**Message:** AFS policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup tar log for additional failure information.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2816

**Message:** DataStore policy restore error

**Explanation:** An error caused the restore of the DataStore data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. If you run one PureDisk disaster recovery, check the output from the `/opt/pdinstall/DR_Restore_all.sh` script on the PureDisk node. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check ownership and permission on the database instance that you restore.
- Check the NetBackup `exten_client` log for additional failure information.



- If you restore a Netezza appliance, collect the log files from `/nz/kit/log/restoresvf/*`.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2817

**Message:** FlashBackup Windows policy restore error

**Explanation:** An error caused some or all of the files to fail the restore operation.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup `tar` log for additional failure information.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2818

**Message:** NetBackup Catalog policy restore error

**Explanation:** An error caused the restore of the NetBackup catalog to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Ensure that NetBackup is at the same version and patch level as the computer where the catalog image was created.
- Ensure that the path where you restore the catalog is same as when it was backed up.
- Ensure that sufficient disk space exists on the target system where the restore runs.

- Ensure that the current master server host name matches the host name of the computer where the catalog image was created.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup `tar`, `admin`, `bptm`, and `bpbrm` logs for additional failure information.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2819

**Message:** Enterprise Vault policy restore error

**Explanation:** An error caused the restore of the Enterprise Vault data to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Check the NetBackup `tar` log for additional failure information. Also, check the Enterprise Vault server Event Viewer (application and system) for errors or clues.
- Connect to the server where the Enterprise Vault front-end runs. Launch the restore by using the Backup, Archive, and Restore GUI.
- Verify that you launched the restore correctly.  
See the [NetBackup for Enterprise Vault Agent Server Administrator's Guide](#).
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2820

**Message:** NetBackup VMware policy restore error

**Explanation:** An error caused the restore of the VMware policy data to fail, as follows:

- If a virtual CD or DVD ISO is not available on the host where you restore the virtual machine, the restore fails. The vCenter interface may include the following message:

```
Invalid configuration for Device '1'.
```

- If the virtual machine to restore and the virtual machine that contains the hotadd restore host do not reside in the same data center, the restore fails.
- The restore host cannot access the VMware datastore over the selected transport mode. The job log on the restore host may contain messages like the following example:

```
FTL - Virtual machine restore: VxMS initialization failed.
```

- You attempted to restore a file that has a path name longer than 1023 characters. A backup of a Linux virtual machine backs up all files, including those with path names longer than 1023 characters. But you cannot restore the long path-name files individually.
- For the restore, the virtual machine's hardware version (such as 7) is later than the hardware version that the target server supports. If VMware Tools cannot convert the virtual machine's hardware version to an earlier version, the restore fails. Messages similar to the following appear in the detailed status log:

```
Info bpVMutil(pid=6268) INF - vmwareLogger: WaitForTaskCompleteEx:  
The virtual machine version is not compatible with the version of the  
host <hostname>.
```

- You attempted to restore a large virtual machine with one or more VMDKs that are formatted as **Thick Provision Eager Zeroed**. Because of the size of the virtual machine or its VMDKs, creation of the virtual machine may take more than 2 hours. As a result, the restore failed.

**Recommended Action:** Check the job details in the Activity Monitor and take action as dictated by that information, as follows:

- Ensure that an .ISO file that is presented to a virtual machine as a virtual CD or DVD during backup is available on the destination host.
- For a successful hotadd restore, ensure that the two virtual machines are in the same VMware data center.
- Select a different transport mode and retry the restore.
- You cannot restore a file that has a path name longer than 1023 characters.

- If possible, restore the VM to a VMware server that supports the VM's hardware version.
- In Backup, Archive, and Restore, change the restored virtual disk to **Thick Provision Lazy Zeroed** or **Thin Provisioning**.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2821

**Message:** Hyper-V policy restore error

**Explanation:** On a Hyper-V restore operation, a connectivity issue between the Hyper-V host and the media server causes `bptm` to fail to write to the socket.

**Recommended Action:** Try the following:

- Update the NIC drivers and firmware if necessary.
- Ensure that the network hardware between the media server and the client operates properly.
- Add NetBackup processes and directories to the Antivirus Exclusion List since antivirus applications may close the established socket.
- Increase TCP resiliency on the Windows hosts (master servers, media servers, and clients) by setting the `TcpMaxDataRetransmissions` registry key to a value of 10. The default value is 5.

More information is available from Microsoft about the

`TcpMaxDataRetransmissions` registry key:

<http://msdn.microsoft.com/en-us/library/aa915651.aspx>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2826

**Message:** Master server failed to connect to backup restore manager on media server for restore

**Explanation:** A process on the master server cannot connect to a process on a host on the network. This error occurs when the process tries to initiate communication with the server that has the storage unit. This problem can occur during a restore in either a single or a multiple server configuration.

**Recommended Action:** Try the following possible solution in the order presented:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

- From each of the media servers, ping the master server by using the name that is specified in the NetBackup server list. On a UNIX or Linux server, this master is the first SERVER entry in the `bp.conf` file. On a Windows server, the master is designated on the **Servers** tab in the **Master Server Properties** dialog box.
- Check that all of the services are running on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2827

**Message:** Client failed to connect to the media server for restore

**Explanation:** The client cannot connect to the media server for a restore operation.

**Recommended Action:** Try the following possible solution in the order presented:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
- Check that all services are running on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2828

**Message:** Restore failed because the MS-SQL-Server services are down

**Explanation:** The SQL Server services are down on the system where the NetBackup client and the NetBackup for SQL Server agent are running. So the NetBackup for SQL Server agent cannot connect to the SQL Server.

**Recommended Action:** Check that the SQL Server instance service is running and that NetBackup processes have permission to access the SQL Server instance service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2829

**Message:** Restore failed due to MS-SQL-Server database in use

**Explanation:** SQL Server database is busy with another operation and cannot restore the requested database on the system where the NetBackup client and the NetBackup for SQL Server agent are running.

**Recommended Action:** After the database finishes its current operation, try to restore the database. Or, the database administrator needs to check if the database is busy and what operation it is performing.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2830

**Message:** Restore failed due to an incorrect path in the MS-SQL-Server MOVE script

**Explanation:** The MOVE template that is generated for the database restore using the NetBackup MS SQL Client has an incorrect path that was specified for the database/log file for the keyword TO.

**Recommended Action:** Check the MOVE script and correct the path that was specified for the database log file for the keyword TO.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2831

**Message:** Restore error

**Explanation:** An error caused the restore to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2832

**Message:** Restore failed due to rename file format error

**Explanation:** The rename file that is used to specify details about virtual machine alternate client location restores cannot be read because it has an invalid format.

**Recommended Action:** If you want to execute the `nbrestorevm` command and manually enter the rename file, verify that the file complies with the format specified in the [NetBackup Commands Reference Guide](#). For additional information, check the job details in the Activity Monitor and the `bprd` log on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2833

**Message:** Restore failed due to partition restore error

**Explanation:** This error is encountered when restoring a raw partition, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2834

**Message:** Restore failed due to failure to read change block bitmap

**Explanation:** NetBackup cannot read the change block bitmap header of the backup image, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2835

**Message:** Restore failed due to corrupt image

**Explanation:** NetBackup reads an invalid backup image header type, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details

in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2836

**Message:** Restore failed because the bitmap size read from the image header differs from the expected size.

**Explanation:** The bitmap size in the backup image header is inconsistent with the bitmap size found in the NetBackup internal database. This failure indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2837

**Message:** Restore failed due to invalid metadata

**Explanation:** Invalid metadata cannot be added to the backup image header, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2838

**Message:** Restore failed because no raw partitions were found

**Explanation:** No raw partitions were found in the backup image, which may indicate that the backup image is defective.

**Recommended Action:** Verify that the backup image contains a list of raw partitions. This error may indicate that the backup image is defective. For additional



information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2839

**Message:** Restore failed due to invalid raw partition ID

**Explanation:** NetBackup cannot identify the raw partition ID, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2840

**Message:** Restore failed due to out of sequence raw partitions

**Explanation:** Raw partition file numbers are out of sequence, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2841

**Message:** Restore failed due to failure to read the header from the backup image

**Explanation:** The restore cannot read the backup image header, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2842

**Message:** Restore failed due to failure to read the VMware bitmap

**Explanation:** The restore operation is unable to retrieve the VMware bitmap from the backup image, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2843

**Message:** Restore failed due to failure to start VxMS

**Explanation:** The restore is unable to load VxMS. VxMS is a library used to map physical addresses of files and volumes.

**Recommended Action:** Verify that the media server and the recovery host environment has adequate memory and correct file permissions. For additional information, check the job details in the Activity Monitor and the `bprd` log on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2844

**Message:** Restore failed due to failure to read the FIID file

**Explanation:** The restore operation is unable to read the FIID file, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2845

**Message:** Restore failed due to failure to retrieve the bitmap

**Explanation:** The restore operation cannot retrieve the backup image bitmap from the NetBackup internal database, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2846

**Message:** Restore failed due to failure to retrieve the fsmap

**Explanation:** The restore operation cannot retrieve the backup image's file system map from the NetBackup internal database, which indicates that the backup image is defective.

**Recommended Action:** If another backup copy exists, make that image the primary copy and attempt to restore from it. For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2847

**Message:** Restore failed due to failure to start the bptm writer

**Explanation:** The restore operation is unable to start the `bptm` writer process.

**Recommended Action:** Verify that the media server and the recovery host environment has adequate memory and correct file permissions. For additional information, check the job details in the Activity Monitor and the `bprd` log on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2848

**Message:** Restore failed due to failure to create the virtual machine

**Explanation:** The following are possible causes:

- Credentials for the VMware server do not have sufficient permissions to create a virtual machine.
- Insufficient space on a datastore.
- Incompatible VM configuration or vmdk configuration.
- Error or task cancelation on the VMware server.

For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

**Recommended Action:** Do the following:

- Check that the VMware server has sufficient permissions.
- Increase the space available for the datastore.
- Resolve any configuration incompatibilities.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2849

**Message:** Restore failed due to failure to delete the virtual machine snapshot

**Explanation:** The restore operation failed due to an error during the delete virtual machine snapshot operation.

**Recommended Action:** Do the following:

- Check that the VMware server has sufficient permissions to delete a virtual machine snapshot.
- Increase the space available for the datastore.
- Error or task cancellation on the VMware server.

For additional information, check the job details in the Activity Monitor, the `bprd` log on the master server, and the `bptm` log on the media server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2850

**Message:** Restore error

**Explanation:** An error caused the restore to fail.

**Recommended Action:** Try the following possible solutions in the order presented:

- Ensure that the client server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
- Correct the problems that you find and retry the restore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2864

**Message:** The disaster recovery package could not be imported.

**Explanation:** The operation was not successful because the disaster recovery package was corrupt.

**Recommended Action:** Ensure that you are using the disaster recovery package that was emailed to you or a copy of the same package.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2865

**Message:** The database table could not be loaded.

**Explanation:** The operation was not successful because the host identity could not be restored in the NetBackup database.

**Recommended Action:** Ensure that the NetBackup database is accessible while the NetBackup database process is running. Use the following command to check if the database is accessible:

- On UNIX: `/usr/opensv/db/bin/nbdb_ping`
- On Windows: `install_path\NetBackup\bin\nbdb_ping`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 2866

**Message:** The specified passphrase is incorrect.

**Explanation:** The operation was not successful, because the passphrase does not match the one that was set at the time of the catalog backup.

**Recommended Action:** Ensure that the specified passphrase is the same as the one that you set at the time of the catalog backup that is associated with this disaster recovery package.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4200

**Message:** Operation failed: Unable to acquire snapshot lock

**Explanation:** The snapshot is being accessed by another operation such as a restore, browse, or copy to storage unit.

**Recommended Action:** Retry the operation when the snapshot is no longer used by another operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4201

**Message:** Incorrect snapshot method configuration or snapshot method not compatible for protecting backup selection entries

**Explanation:** The policy uses an incorrect snapshot method, or the prerequisite for this snapshot method is not configured properly.

**Recommended Action:** Verify the following:

- The required correct storage array credential for the snapshot method (wherever applicable) is configured in NetBackup.
- The required software for the snapshot method is configured correctly on the client.
- You can choose the snapshot method to protect the entries of the backup selection (for example, file system).
- The entries that are specified in the backup selection are compatible with the snapshot method configured in the policy.

See the [NetBackup Snapshot Client Administration Guide](#) for more information about configuring a snapshot method.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4202

**Message:** Invalid or incompatible storage unit configured

**Explanation:** Invalid or incorrect storage destination configured for this policy.

**Recommended Action:** Verify the following:

- The storage destination that is used for the policy is compatible. For example, the snapshot method OST\_FIM operates only on an SLP configured as storage destination.
- The configuration parameter that was provided for the snapshot method is correct. For example, verify that the snapshot resources are correct and the configuration parameters for the configured snapshot method are correct.
- You can choose the snapshot method to protect the entries of the backup selection (for example, file system).  
 See the [NetBackup Snapshot Client Administration Guide](#) for more information about configuring a snapshot method.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4203

**Message:** Invalid or unsupported backup selection filelist

**Explanation:** Incompatible entry found in backup selection for the configured snapshot method.

**Recommended Action:** Verify the following:

- The entries that are given in the backup selection can be protected by the snapshot method. For example, a file system that was created on top of an HP EVA disk cannot be protected using the snapshot method for IBM.
- The volume is mounted on the specified path for NAS volumes (NFS mount points or CIFS share).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4204

**Message:** Incompatible client found

**Explanation:** Invalid user on client or incompatible client found.

**Recommended Action:** Verify the following:

- You have logged into the client with the same domain-user as the one registered with the NetBackup client service.
- The primary client and target or remote client are compatible.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4205

**Message:** Incorrect or no credentials found

**Explanation:** Either NetBackup cannot find the supporting software for the configured snapshot method or invalid credentials have been supplied.

**Recommended Action:** Verify the following:

- If you created an NDMP policy or configured an NAS Data Mover, check that the NDMP host is configured with the correct credentials.
- The disk array host or storage server credentials are correct.
- The third party software or supporting software that is required by the configured snapshot method is installed on the client.  
See the [NetBackup Snapshot Client Administration Guide](#) for more information about snapshot methods.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4206

**Message:** Authentication error occurred. NetBackup Client Service is running as Local System, this is likely incorrect.

**Explanation:** None of the backup selections are accessible and the NetBackup Client Service is running as Local System. These conditions indicate that you may not have credentials to access the storage server.

**Recommended Action:** Update the NetBackup Client Service in the Windows services to use the proper credentials that allow access to the storage server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4207

**Message:** Could not fetch snapshot metadata or state files



**Explanation:** Snapshot metadata that the NetBackup client requires is missing or cannot be fetched from the NetBackup master server.

**Recommended Action:** Verify the following:

- The NetBackup client can communicate with the NetBackup master.
- The state file location on the NetBackup client has write permission. The typical location of the NetBackup state file on the NetBackup client is as follows:  
Windows: `C:\Program Files\Veritas\NetBackup\online_util\fi_cntl\`  
UNIX: `/usr/opensv/netbackup/online_util/fi_cntl`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4208

**Message:** Could not send snapshot metadata or statefiles

**Explanation:** Snapshot metadata that is created by the client cannot be transferred on the master server.

**Recommended Action:** Verify the following:

- The NetBackup client can communicate with the NetBackup master.
- The state file location on the NetBackup client has write permission. The typical location of the NetBackup state file on the NetBackup client is as follows:  
Windows: `C:\Program Files\Veritas\NetBackup\db\snapshot\<client>`  
UNIX: `/usr/opensv/netbackup/db/snapshot/<client>`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4209

**Message:** Snapshot metadata or statefiles cannot be created

**Explanation:** Not able to create snapshot metadata.

**Recommended Action:** Verify the following:

- The logs contain a failure that precedes this error which restricts the creation of metadata content.
- The state file location on the NetBackup client has write permission. The typical location of the NetBackup state file on the NetBackup client is as follows:  
Windows: `C:\Program Files\Veritas\NetBackup\db\snapshot\<client>`  
UNIX: `/usr/opensv/netbackup/db/snapshot/<client>`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4210

**Message:** Incorrect or no content found in snapshot metadata

**Explanation:** Incorrect or invalid content in the snapshot state files.

**Recommended Action:** Verify that the specified state file is present on the host. The NetBackup state file is normally located in the following NetBackup client directory:

- Windows: C:\Program Files\Veritas\NetBackup\online\_util\fi\_cntl\
- UNIX: /usr/opensv/netbackup/online\_util/fi\_cntl

Contact Veritas NetBackup support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4211

**Message:** Snapshot not accessible or invalid snapshot

**Explanation:** The snapshot is not accessible. The target device may be mapped to multiple host bus adapters (HBAs).

**Recommended Action:** Verify the following:

- The connection between the NetBackup client and the storage management host-array is intact.
- The host-specific permission is enabled on the storage array.
- The snapshot exists on the storage array or filer.
- The snapshot target device is not mapped to multiple HBAs. If it is, unmap one of the HBAs and continue. Support of multiple paths for a device that requires the multi-path software.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4212

**Message:** Recreation of snapshot failed

**Explanation:** Snapshot cannot be recreated. This error can occur during snapshot restores on a Windows platform.

**Recommended Action:** Verify that the restore flow of operations has succeeded.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4213

**Message:** Snapshot import failed

**Explanation:** The snapshot import operation failed, or building and enabling the snapshot I/O stack failed.

**Recommended Action:** Verify the following:

- The snapshot device is accessible on the client.
- The client has all the required software for building the snapshot I/O stack. This should be equivalent to the I/O stack of the primary client whose entity was required to be protected.
- The communication between the NetBackup client and the master server is intact.
- The copy-back restore target device is not mapped to multiple HBAs. If it is, unmap one of the HBAs and continue. Support of multiple paths for a device requires the multi-path software.
- Make sure that the iSCSI session is established between the node and the target.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4214

**Message:** Snapshot mount failed

**Explanation:** Unable to mount the snapshot or run the subsequent set of snapshot operations. The user needs to make the snapshot accessible to the next set of operations to complete a NetBackup job (for example, backup from snapshot, indexing, restore wherever applicable).

**Recommended Action:** Verify the following:

- You can use the required file system type to mount the given snapshot.
- The required permission exists on the client to enable snapshots for reading and traversing.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4215

**Message:** Snapshot deletion failed

**Explanation:** The snapshot cannot be deleted.

**Recommended Action:** Verify the following:

- The snapshot exists on the storage array. It may have been deleted outside of NetBackup.
- The client has permission to delete the snapshot.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4216

**Message:** Snapshot cleanup failed

**Explanation:** Unable to clean up various supporting pieces for snapshot creation.

**Recommended Action:** Verify that you have enabled the permission to delete the files.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4217

**Message:** Snapshot restore failed

**Explanation:** Unable to restore data from the snapshot.

**Recommended Action:** Verify the following:

- The snapshot exists.
- You have enough permission to overwrite or create files in the restore directory or folder.
- The communication between NetBackup and the storage array-filer is intact.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4218

**Message:** Snapshot deport failed

**Explanation:** The requested snapshot cannot be deported or masked from the NetBackup client.

**Recommended Action:** Verify the following:

- The snapshot exists.
- The communication between NetBackup and the storage array-filer is intact.
- The required credentials for the storage server have been supplied in NetBackup.
- Any required software and license for the third-party software are configured.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4219

**Message:** Command operation failed: Third-party command or API execution failed

**Explanation:** Third-party command or API execution failed.

**Recommended Action:** Do the following:

- From the NetBackup logs, identify the failing command or API.
- Ensure that you have the required permission to execute these commands.
- If possible, execute the command manually to gather more details about the failure.
- Check your configuration to determine the cause of the failing command or the API.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4220

**Message:** Command operation failed: System command or API execution failed

**Explanation:** The system command or the API execution failed.

**Recommended Action:** Verify the following:

- From the NetBackup logs, identify the failing command or API.
- Take corrective actions based on the error that is reported as a result of the command execution.
- Ensure that you have the required permission to execute these commands.
- If possible, execute the command manually to gather more details about the failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4221

**Message:** Found an invalid or unsupported configuration

**Explanation:** NetBackup found an invalid or unsupported configuration.

**Recommended Action:** Verify the following:

- From the NetBackup logs, identify the failing entity and its error.
- Check the support matrix to determine the correct setup for the configuration.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4222

**Message:** Operation failed: Unable to acquire policy lock to take snapshot

**Explanation:** A policy has generated overlapping snapshot jobs. One snapshot job is in progress for a particular policy when the same policy requests a second snapshot job.

**Recommended Action:** No manual intervention is required. The NetBackup Policy Execution Manager (PEM) retries the job based on the **Job retry delay** setting on the master server. To view or set this property, go to **Host Properties>Master Server>Global Parameters**. Contact NetBackup Support if you continue to get this error and you have ensured that no overlapping snapshot jobs are in progress.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4223

**Message:** Operation not completed

**Explanation:** The user runs the `nbrestorevm -ir_done` command to complete the VM Instant Recovery operation, but the VM continues to run from the NetBackup storage. The operation cannot be completed because Storage vMotion may be running or not started.

**Recommended Action:** Make sure that Storage vMotion is completed and that you move the VM from NetBackup storage to the production datastore.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4224

**Message:** STS Internal Error

**Explanation:** One of the following has occurred inside the STS plug-in:

- Insufficient system memory in the client or the storage server.
- Storage server busy.
- An invalid request was received in the communication between the storage server and the STS plug-in.

**Recommended Action:** Please contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4225

**Message:** Unauthorized operation attempted by client or media on storage server

**Explanation:** The storage server received an unauthorized request or did not identify the host.

**Recommended Action:** Verify the following:

- Valid storage server credentials are configured.
- The client has the required privileges per the vendor specification. Please refer to the [NetBackup Replication Director Solutions Guide](#) for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4226

**Message:** Communication failure occurred with storage server

**Explanation:** NetBackup cannot communicate with the storage server or a protocol failure has occurred with the storage server.

**Recommended Action:** Verify the following:

- The appropriate storage server services are running.
- The client and the media server can communicate with the storage server.
- The client and the media server can resolve the storage server name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4227

**Message:** STS Plug-in error occurred

**Explanation:** The STS plug-in framework is not working.

One of the following has occurred:

- A required STS library cannot be loaded or initialized.
- An invalid plug-in operation is attempted.

**Recommended Action:** Please contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4228

**Message:** Storage server or plug-in version mismatch

**Explanation:** The STS plug-in framework encountered an incompatible storage server version.

**Recommended Action:** Verify that the client and the media server support the version of the storage server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4229

**Message:** Insufficient resources or capabilities found by storage server

**Explanation:** The storage server does not have sufficient resources or capabilities available. For example, not enough space exists on the storage that the storage server manages. Also, appropriate feature licenses are not enabled on the storage server.

**Recommended Action:** Verify the following:

- The storage server recognizes the identified device from the backup selection.
- The required features are enabled on the storage.
- The required feature licenses are applied on the storage.
- The storage server has sufficient available storage space for NetBackup triggered snapshots.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4230

**Message:** Invalid storage topology or storage server configuration error



**Explanation:** An invalid configuration causes the STS Plug-in to fail. Examples of this failure include an invalid topology configuration, storage configuration, or server configuration.

**Recommended Action:** Do the following:

- Verify that the storage is correctly configured per the vendor specification.
- Verify that the underlying storage supports the topology that is specified in the storage lifecycle policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4231

**Message:** STS Unexpected Error

**Explanation:** The STS Plug-in failed with an unexpected error.

**Recommended Action:** Please contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4232

**Message:** Invalid Discovery Query URI

**Explanation:** The query URI for the discovery policy cannot be parsed.

**Recommended Action:** Examine the URI using the policy editor for syntax errors.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4233

**Message:** BIOS UUID client reference not allowed for vCloud

**Explanation:** Use of BIOS UUID as a client reference is not allowed for vCloud because they are not unique.

**Recommended Action:** Select another form of client reference for the policy, possibly instance UUID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4234

**Message:** VMware server login failure

**Explanation:** The configured user name, password, and port do not allow login to the server.

**Recommended Action:** Correct the credentials that are configured for the designated server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4235

**Message:** vCloud keyword used when vCloud not enabled

**Explanation:** The policy uses a vCloud related keyword, but a vCloud server credential is not configured.

**Recommended Action:** Configure a vCloud director credential, or remove any vCloud related keywords from the policy query.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4236

**Message:** vCloud policy includes multiple organizations

**Explanation:** Executing the query for the policy selected VMs from multiple vCloud organizations and this has not been enabled in the policy.

**Recommended Action:** Correct the policy query to select only VMs from a single organization, or change the policy to enable VMs from multiple organizations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4237

**Message:** Client does not meet policy requirements

**Explanation:** The VM cannot be backed up because it does not meet the requirements for the selected client reference.

**Recommended Action:** Modify the VM to meet the requirements for the configured client reference, or change the policy to use a different client reference.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4238

**Message:** No server credentials configured for policy

**Explanation:** The discovery policy requires credentials for a server to execute the policy.

**Recommended Action:** Verify that the appropriate server credentials have been entered for the type of discovery policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4239

**Message:** Unable to find the virtual machine

**Explanation:** Possible causes of this error:

- The virtual machine name is not entered correctly (for example, the name is misspelled).
- The virtual machine identifier type is not selected correctly for the policy. For example, the virtual machine display name is entered, but the virtual machine identifier for the policy indicates virtual machine host name.
- The virtual machine is renamed, deleted, or moved.

**Recommended Action:** Verify the following:

- The virtual machine identifier configured for the policy and the name (display name, host name, UUID) entered for the virtual machine on the policy agree.
- You can view the virtual machine in the VMware user interface.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4240

**Message:** Operation not supported

**Explanation:** A likely cause is a Veritas programming error.

**Recommended Action:** Please contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4243

**Message:** Unable to connect to the VirtualCenter server

**Explanation:** The connection to the VirtualCenter server cannot be made. Possible causes of this error:

- If there are too many VM snapshot jobs that are started using the same VirtualCenter server, the VirtualCenter server connection limit is exceeded.
- There is an intermittent network connection between the VMware backup host and the VirtualCenter server.

**Recommended Action:** If there are too many VM snapshot jobs, limit the VM jobs using the VMware Resource Limit to limit the concurrent jobs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4245

**Message:** Invalid pathname for backup selection

**Explanation:** NDMP pathname for NetApp clustered Data ONTAP is expected with the format `/vserver_name/vol_name`.

**Recommended Action:** The IP address cannot be used in the pathname.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4246

**Message:** The requested operation was partially successful.

**Explanation:** Potential causes of this error are:

- Not all backup selections apply to all selected clients
- The backup selection refers to an invalid volume name
- The backup selection refers to a directory

**Recommended Action:** Do the following:

- Create a separate policy for each client
- Specify the correct volume name for the Vserver
- Specify a volume name and not a directory within a volume

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4247

**Message:** Index from snapshot for Replication Director NDMP Policy is not supported on AIX media server

**Explanation:** Index from the snapshot for Replication Director NDMP Policy is supported only on Linux, Windows, HP-UX, and the Solaris media server.

**Recommended Action:** Please associate a supported media server other than the AIX media server for the storage unit referred to in the SLP against the index from the snapshot operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4248

**Message:** Index from snapshot operation failed with an internal error

**Explanation:** Index from snapshot operation failed with an internal error.

**Recommended Action:** Check the NetBackup administration logs for more details. Ensure that there is enough space on the media server to create the index database.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4249

**Message:** Index from snapshot operation failed, catalog already exists

**Explanation:** Index from snapshot operation fails when there already is a full catalog created for the given source image.

**Recommended Action:** Check that there is no existing catalog for the specified source image. Check the NetBackup administration logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4250

**Message:** Index from snapshot operation failed, unable to find child image or file information

**Explanation:** Index from snapshot operation failed. No child images found for the backup ID that needs to be indexed.

**Recommended Action:** Check the NetBackup administration logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4251

**Message:** Index from snapshot operation failed. Failed to write into index database.

**Explanation:** Error occurred on media server while writing into index database.

**Recommended Action:** Typically, the index database is created under `NB_INSTALL_DIR/tmp`; for example, `/usr/opensv/netbackup/tmp`. It can be overridden by `SNAPDIFF_DB_PATH` in the NetBackup configuration file. Ensure that there is enough space on the media server to create the index database. Check the NetBackup administration logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4252

**Message:** Index from snapshot operation failed. Entry does not belong to any of the backup selection entries.

**Explanation:** The file entry going to be indexed does not belong to any of the backup selection entries.

**Recommended Action:** Check the NetBackup administration logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4253

**Message:** Index from snapshot operation failed. SLP version mismatch for current and previous backup image.

**Explanation:** Index from snapshot operation failed. There is an SLP version mismatch for the current and previous backup image.

**Recommended Action:** Check the NetBackup administration logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4254

**Message:** Invalid or no path found to create index database

**Explanation:** There is an invalid path or no path to create the index database. This path is required to create an index database in an index from snapshot operation.

**Recommended Action:** Typically, the index database is created under `NB_INSTALL_DIR/tmp`; for example, `/usr/opensv/netbackup/tmp`. It can be overridden by adding `SNAPDIFF_DB_PATH` in the NetBackup configuration. Check if the defined path exists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4255

**Message:** Index from snapshot using SnapDiff is disabled by the user

**Explanation:** The user can disable the index from snapshot operation by using SnapDiff through the NetBackup configuration key `USE_SNAPDIFF`. If the value of the key is set to 0, then the index from the snapshot operation using SnapDiff is disabled.

**Recommended Action:** To enable the index from snapshot by using SnapDiff, change the value of the NetBackup configuration key `USE_SNAPDIFF` by using the `bpsetconfig` CLI. The possible values of the key are as follows:

- Set to 0; do not perform the index from snapshot operation by using SnapDiff.
- Set to 1; the index from snapshot by using SnapDiff is enabled only for the incremental schedule.
- Set to 2; the index from snapshot by using SnapDiff is enabled for all schedule types.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4256

**Message:** Index from snapshot is not supported for the file system associated with backup selection

**Explanation:** The index from snapshot is not supported for the file system associated with one of the backup selection entries.

**Recommended Action:** Currently, the index from the snapshot operation using SnapDiff is supported for NFS, CIFS file systems. It is also supported when the policy type is NDMP. Change the policy with the backup selection entries that have a file system that is supported for the index from snapshot operations by using SnapDiff.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4257

**Message:** Index from snapshot is not supported for the storage server

**Explanation:** Index from snapshot using SnapDiff is not supported for the storage server that is used for snapshot creation.

**Recommended Action:** Please check that the index from snapshot using SnapDiff is supported for the storage server. If it is not, then change the SLP with the STU associated with the storage server having support for index from snapshot using SnapDiff.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4258

**Message:** Transient error encountered while taking Hyper-V VM snapshot

**Explanation:** The Hyper-V VSS writer experienced a transient error. VM might be moving or doing another conflicting operation. If the backup process is retried, the error may not reoccur.

**Recommended Action:** Check the event log for Hyper-V VMMS (Log Name: Microsoft-Windows-Hyper-V-VMMS/Admin) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4259

**Message:** Failed to find VirtualCenter host name in VMware Lookup Service

**Explanation:** The Platform Services Controller system name for the vCenter cannot be resolved to the NetBackup virtual machine server name for a vCenter.

**Recommended Action:** Use the system name as configured in the Platform Services Controller as the NetBackup virtual machine server name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4260

**Message:** Encountered SSO login failure



**Explanation:** Login failed when attempting to log on to the VMware Single Sign-On service.

**Recommended Action:** Ensure that the credentials that you entered for the NetBackup virtual machine server are authorized for Single Sign-On.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4261

**Message:** Encountered VMware Internal Server Error

**Explanation:** This message indicates a generic VMware Internal Server Error. A known cause of this error is when the Tags or Categories that are defined in the vCenter do not have a Description.

**Recommended Action:** Refer to the details that are given in the error message and the related VMware Knowledge Base article. Check the NetBackup VxUL logs (`libvcloudsuite`).

Related VMware Knowledge Base article: <http://kb.vmware.com/kb/2124204>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4262

**Message:** Encountered VMware vCloud Suite API failure

**Explanation:** This message indicates a generic VMware API failure. A known cause of this error is when NetBackup master servers or other hosts that perform automatic virtual machine selection do not have network connectivity to the VMware Platform Services Controller.

**Recommended Action:** Refer to the *VMware vCenter Server 6.0 Deployment Guide* and the related VMware Knowledge Base article.

Related VMware Knowledge Base article: <http://kb.vmware.com/kb/2106283>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4263

**Message:** Encountered VMware SOAP API failure

**Explanation:** This message indicates an error when NetBackup attempted to connect to the VMware Single Sign-On service. A known cause of this error is when

the clock settings are different between the NetBackup host that is used for virtual machine selection and the vCenter.

**Recommended Action:** Refer to the details that are given in the error message and the related VMware Knowledge Base article. Check the NetBackup VxUL logs (`libvcloudsuite`).

VMware Knowledge Base article: <http://kb.vmware.com/kb/2125193>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4264

**Message:** Encountered unexpected error while processing TagView XML

**Explanation:** This message indicates that the XML file containing the VMware Tag information is corrupt.

**Recommended Action:** If the error is from a test query, try the operation again. If the parent (Discovery) job fails, try the job again with a **Reuse VMware selection query results** value of 0 in the failing policy clients tab to regenerate the XML file.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4265

**Message:** Encountered a VMware Virtual Machine Server that does not support Tags

**Explanation:** This message indicates that an ESX server is included in the Virtual Machine Server list, which does not support Tags.

**Recommended Action:** Refer to the [NetBackup for VMware Administrator's Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4266

**Message:** Encountered a VMware Virtual Machine Server that does not offer Tag APIs

**Explanation:** This message indicates that a 5.1 or 5.5 vCenter is included in the Virtual Machine Server list, which does not offer VMware Tag APIs.

**Recommended Action:** Refer to the [NetBackup for VMware Administrator's Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4267

**Message:** Failed to initialize Java Runtime Environment

**Explanation:** This error message indicates that NetBackup cannot find the Java Runtime Environment that is required to access the VMware Tag information.

**Recommended Action:** Install the version of the NetBackup Remote Administration Console that corresponds to the NetBackup Client installation. The version of the NetBackup Remote Administration Console must match the NetBackup Client version.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4268

**Message:** Failed to retrieve resource pool information

**Explanation:** NetBackup was not able to retrieve resource pool properties from vSphere.

**Recommended Action:** Check the resource pool path. If it is incorrect, specify the correct resource pool path that exists in destination vCenter server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4269

**Message:** Found multiple virtual machines with same identity

**Explanation:** Multiple virtual machines with the same display name exist under the destination resource pool or vApp. NetBackup cannot identify the virtual machine that needs to be overwritten.

**Recommended Action:** Select a different display name for restore or rename the virtual machines in the destination resource pool or vApp. Only one virtual machine with the same display name can exist in the resource pool or vApp.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4270

**Message:** A snapshot of the virtual machine exists and the policy option specifies aborting the backup

**Explanation:** The virtual machine being backed up already has an existing snapshot and the backup policy requires that NetBackup abort the backup in this circumstance.

**Recommended Action:** Either remove the snapshot and restart the backup job or modify the policy to ignore or remove existing snapshots. NetBackup removes existing snapshots only if NetBackup created them.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4271

**Message:** Maximum virtual machine snapshots exceeded

**Explanation:** NetBackup was unable to remove an existing virtual machine snapshot because more than the maximum allowed number of snapshots exist on the virtual machine.

**Recommended Action:** Remove the virtual machine's snapshots and restart the backup job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4272

**Message:** Maximum delta files exceeded

**Explanation:** One of the virtual machine's disks had more than the maximum allowed number of delta files. Therefore, NetBackup was unable to create a virtual machine snapshot.

**Recommended Action:** Consolidate the virtual machine's disks and restart the backup job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4273

**Message:** Unable to lock the backup or restore host for virtual machine snapshot operations

**Explanation:** NetBackup was configured to serialize the virtual machine snapshot operations on the backup or restore host. However, NetBackup was unable to acquire the lock that controls snapshot serialization within the allowed time.

**Recommended Action:** Restart the backup job when no other virtual machine snapshot operations are in process. If NetBackup cannot acquire the lock frequently, adjust the NetBackup job configuration as necessary to allow the virtual machine snapshots to run at different times or to run on different hosts. Alternatively, reconfigure NetBackup so that the snapshot serialization is not required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4274

**Message:** Failed to remove virtual machine snapshot

**Explanation:** NetBackup was unable to remove a virtual machine snapshot.

**Recommended Action:** Delete the virtual machine snapshot manually.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4275

**Message:** Unable to consolidate Virtual Machine Disks

**Explanation:** NetBackup was unable to consolidate a virtual machine's disks. NetBackup tries to consolidate disks as follows:

- Before a virtual machine snapshot is created at the start of a virtual machine backup.
- After a virtual machine snapshot is deleted while the backup nears completion.

**Recommended Action:** Consolidate the virtual machine's disks manually and restart the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4276

**Message:** Unable to retrieve Virtual Machine Disk information

**Explanation:** NetBackup was unable to retrieve a virtual machine's disk information.

**Recommended Action:** Review the job details and the `bpfis` log for any additional information that is related to the error. Correct the underlying issues that cause the failure and restart the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4277

**Message:** Virtual machine path contains unsupported characters

**Explanation:** The virtual machine path contains the characters that NetBackup does not support.

**Recommended Action:** Rename the virtual machine and/or folder path to one that contains only supported characters.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4278

**Message:** Unable to retrieve virtual machine information

**Explanation:** NetBackup was unable to retrieve a virtual machine's information.

**Recommended Action:** Review the job details and the `bpfis` log for any additional information that is related to the error. Correct the underlying issues that cause the failure and restart the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4279

**Message:** Unable to retrieve virtual machine vCloud information

**Explanation:** NetBackup was unable to retrieve a virtual machine's vCloud information.

**Recommended Action:** Review the job details and the `bpfis` log for any additional information that is related to the error. Correct the underlying issues that caused the failure and restart the job.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4280

**Message:** Virtual machine contains independent and Raw Device Mapping disks only

**Explanation:** The virtual machine included only independent disks and the Raw Device Mapping disks, so NetBackup found no data to protect.

**Recommended Action:** Remove the virtual machine from the backup policy selection or modify the virtual machine to include additional disks.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4281

**Message:** Virtual machine contains independent disks only

**Explanation:** The virtual machine included only independent disks, so NetBackup found no data to protect.

**Recommended Action:** Remove the virtual machine from the backup policy selection or modify the virtual machine to include additional disks.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4282

**Message:** Virtual machine contains Raw Device Mapping disks only

**Explanation:** The virtual machine included only Raw Device Mapping disks, so NetBackup found no data to protect.

**Recommended Action:** Remove the virtual machine from the backup policy selection or modify the virtual machine to include additional disks.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4283

**Message:** Error detected while processing disk identifiers

**Explanation:** NetBackup encountered more than one Virtual Machine Disk with the same UUID.

**Recommended Action:** Modify the virtual machine so that none of the UUIDs for its disks duplicate the UUID for any other virtual machine.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4287

**Message:** A NetBackup snapshot of the virtual machine exists and the policy option specifies aborting the backup

**Explanation:** One or more NetBackup created snapshots exist on the virtual machine and the **Existing snapshot handling** option in the policy specifies aborting the backup. The snapshots that NetBackup creates start with the `NBU_SNAPSHOT` or `NBU_RESTORE` strings in the snapshot name.

Possible causes of an existing NetBackup snapshot are the following:

- A snapshot from a previous backup has not been deleted (an orphaned snapshot). NetBackup should have deleted the snapshot when the backup completed.
- Two policies try to back up the virtual machine at the same time. The backup for one of the policies detects the snapshot that the other policy created.

**Recommended Action:** Do the following, as appropriate:

- Manually remove the orphaned snapshot.  
For VMware, you can use the VMware vSphere interface to remove virtual machine snapshots. For Hyper-V, you can use `nbhypervtool.exe` to remove NetBackup snapshots that were created with the WMI backup method. For more information on `nbhypervtool.exe`, refer to the [NetBackup Commands Reference Guide](#).
- Reduce the likelihood of orphaned snapshots by changing the resource limits to reduce the load on the appropriate VMware or Hyper-V resource. The **Resource Limit** dialog is in the **NetBackup Administration Console** under **Host Properties > Master Servers**. The NetBackup guides for VMware and Hyper-V describe the available settings.
- Change the NetBackup policy schedules to avoid simultaneous backups of the virtual machine.
- For VMware only: Change the NetBackup policy's **Existing snapshot handling** parameter to a different option (such as **Continue Backup**).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 4290

**Message:** Failed to create virtual machine snapshot. Virtual machine is busy performing another operation.

**Explanation:** A virtual machine snapshot cannot be created because the virtual machine is performing another operation that conflicts with the snapshot creation process. This usually happens if the virtual machine is undergoing a storage migration or a live migration.

**Recommended Action:** Retry the snapshot job after the virtual machine has completed the conflicting operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4293

**Message:** Invalid credentials or an access violation

**Explanation:** The credentials that were provided while accessing the host/server are invalid or the host/server denied the access. The requested operation cannot be completed.

**Recommended Action:** Verify that there are valid credentials configured for the host/server that is being accessed and that the user has valid privileges to make the request.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 4294

**Message:** The virtual machine is disconnected

**Explanation:** The ESXi host is disconnected from the virtual machine.

**Recommended Action:** Ensure that the ESXi host is powered on and the vCenter Server agent (vpxa) is running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5400

**Message:** Backup error - None of the request objects were found in the database

**Explanation:** The backup selection list did not contain any objects that were found in the database. An object can either be a data file or a tablespace.

**Recommended Action:** Check the backup selection list. Add the objects that are part of the database or remove the database instance from the policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5401

**Message:** Backup error - FRA (Fast Recovery Area) was requested, but it was not found in the database

**Explanation:** The backup request was for the FRA, but the FRA was not found in the database.

**Recommended Action:** Add an FRA area to the database or remove the database instance from the policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5402

**Message:** OS Authentication error - Could not connect to the database. Please check the OS credentials

**Explanation:** A connection to the database cannot be established using the operating system credentials provided.

**Recommended Action:** Confirm that the credentials are properly set. On Windows, you may need to replace a process level token. First, select **Start>Control Panel>Administrative Tools>Local Security Policy**. Then, expand **Local Policies** in the left pane, click **User Rights Assignment**, and double-click **Replace a process level token** in the right pane. Add the user you want to run the client policies as. Restart the server for this right to take effect.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5403

**Message:** Oracle Authentication error - Could not connect to the database. Please check the Oracle credentials

**Explanation:** A connection to the database cannot be established using the Oracle database credentials that are provided.

**Recommended Action:** Confirm that the credentials are properly set.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5404

**Message:** ASM validation error - PROXY backup is not supported for ASM

**Explanation:** The backup request was for a PROXY type of backup. Automatic Storage Management (ASM) was found. Proxy backups are not supported with ASM.

**Recommended Action:** Move the database to non-ASM storage or remove the database instance from the policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5405

**Message:** Recovery Catalog Authentication error - Could not connect to the Recovery Catalog. Please check the Recovery Catalog credentials.

**Explanation:** A connection to the Recovery Catalog database cannot be established using the Recovery Catalog credentials provided.

**Recommended Action:** Confirm that the Recovery Catalog credentials are properly set.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5406

**Message:** Archive log only backup requested, but database is not in ARCHIVELOG Mode

**Explanation:** The requested operation requires that the database archive log mode to be set to ARCHIVELOG mode or MANUAL mode.

**Recommended Action:** Confirm that the database archive log mode is properly set to either ARCHIVELOG or MANUAL.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5407

**Message:** Database is in the wrong state (must be OPEN) for the requested action

**Explanation:** The requested operation requires that the database be in an OPEN mode.

**Recommended Action:** Confirm that the database mode is set to OPEN. Possible Oracle commands startup, startup open read only, or startup open.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5408

**Message:** OS Authentication error - Could not find credentials. If this instance is part of an instance group, make sure that the group has the credentials that match this OS Type

**Explanation:** The credentials that are needed to connect to the instance cannot be found.

**Recommended Action:** If the instance is on a UNIX client, make sure that its instance group contains UNIX credentials. If the instance is on a Windows client, make sure that its instance group contains Windows credentials.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5409

**Message:** Cloning is NOT supported for this client platform

**Explanation:** The platform that runs on this client does not support the Guided Recovery cloning operation.

**Recommended Action:** Refer to the release notes or the NetBackup Master Compatibility List for the supported platforms for the cloning feature at the following URL:

<http://www.netbackup.com/compatibility>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5410

**Message:** Oracle Intelligent Policy is NOT supported for this client platform

**Explanation:** The platform that runs on this client does not support the Oracle Intelligent Policy feature.

**Recommended Action:** Refer to the release notes or the NetBackup Master Compatibility List for the supported platforms for this feature at the following URL:

<http://www.netbackup.com/compatibility>

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5411

**Message:** Cannot do a hot backup of a database in NOARCHIVELOG mode

**Explanation:** The requested operation requires the database archive log mode to be set to ARCHIVELOG mode.

**Recommended Action:** Confirm that the database archive log mode is properly set to ARCHIVELOG or change to an offline (cold) database backup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5412

**Message:** Database is in the wrong state (must be OPEN or MOUNTED) for an Archive Log Backup

**Explanation:** An Oracle policy requests an archive log backup, but the database is not in an OPEN or MOUNTED state.

**Recommended Action:** Put the database in an OPEN or MOUNTED state and retry the backup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5413

**Message:** Database is in the wrong state (must be OPEN or MOUNTED) for an FRA backup

**Explanation:** An Oracle policy requests a Fast Recovery Area (FRA) backup, but the database is not in an OPEN or MOUNTED state.

**Recommended Action:** Put the database in an OPEN or MOUNTED state and retry the backup.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5414

**Message:** The requested operation is not supported with this client version

**Explanation:** The requested operation is not supported by this version of the NetBackup Client service.

**Recommended Action:** Upgrade the NetBackup Client service to enable this operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5415

**Message:** Cannot shut down read-only standby database

**Explanation:** NetBackup does not perform a cold backup on a standby database that is in read-only mode.

**Recommended Action:** Do not select the cold database backup option on the **Oracle** tab of the policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5416

**Message:** Oracle cannot resolve the TNS connection identifier

**Explanation:** Oracle cannot resolve the TNS connection ID, so NetBackup doesn't know which database to connect to.

**Recommended Action:** Verify the following:

- The correct TNS identifier.
- The correctly configured **tnsnames.ora** file.
- The correct path for the TNS\_ADMIN environment variable.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5417

**Message:** An error has occurred checking if the NFS server is an appliance.

**Explanation:** NetBackup cannot verify that the database backup share is on an appliance.

**Recommended Action:** Verify that the database backup share is exported from a NetBackup appliance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5418

**Message:** The NFS server is not an appliance.

**Explanation:** The database backup share is not located on an appliance.

**Recommended Action:** Verify that the database backup share is exported from a NetBackup appliance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5419

**Message:** The database backup share directory is not available on the appliance.

**Explanation:** NetBackup cannot access the database backup share directory on the appliance.

**Recommended Action:** Verify that the database backup share directory exists on the NetBackup appliance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5420

**Message:** Whole Database - Datafile Copy Share selection is not supported for this client platform.

**Explanation:** Snapshot Client is not supported on this platform so we cannot support it for the Whole Database - Datafile Copy Share selection.

**Recommended Action:** Back up the database using a different method.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5421

**Message:** None of the requested pluggable databases were found.

**Explanation:** The backup request for the database was for a specific list of pluggable databases. This list of pluggable databases was verified in the database and none of the requested pluggable databases were found in the database.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of the pluggable databases that are specified in the Oracle Intelligent Policy are correct and in the requested database. Update the list of pluggable databases in policy. If the pluggable databases were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5422

**Message:** Partial success - one or more of the requested pluggable databases were not found.

**Explanation:** The backup request for the database was for a specific list of pluggable databases. This list of pluggable databases was verified in the database and one or more of the requested pluggable databases were not found in the database. The databases found were backed up.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of pluggable databases that are specified in the Oracle Intelligent Policy are correct and in the requested database. Update the list of pluggable databases in policy. If the pluggable databases were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5423

**Message:** None of the requested tablespaces were found in the requested pluggable databases.

**Explanation:** The backup request for the database was for specific lists of pluggable databases and tablespaces. These lists were verified in the database and none of the requested tablespaces were found in any of the requested pluggable databases.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of tablespaces that are specified in the Oracle Intelligent Policy are correct and in the requested pluggable databases. Update the lists, where applicable, in policy. If the pluggable databases or



tablespaces were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5424

**Message:** Partial success - one or more of the requested pluggable databases did not contain any of the requested tablespaces.

**Explanation:** The backup request for the database was for specific lists of pluggable databases and tablespaces. These lists were verified in the database and one or more of the requested pluggable databases did not contain any of the requested tablespaces. The tablespaces that were found in the pluggable databases were backed up.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of tablespaces that are specified in the Oracle Intelligent Policy are correct and in the requested pluggable databases. Update the lists, where applicable, in policy. If the pluggable databases or tablespaces were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5425

**Message:** None of the requested data files were found in the requested pluggable databases.

**Explanation:** The backup request for the database was for specific lists of pluggable databases and data files. These lists were verified in the database and none of the requested data files were found in any of the requested pluggable databases.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of data files that are specified in the Oracle Intelligent Policy are correct and in the requested pluggable databases. Update the lists, where applicable, in policy. If the pluggable databases or data files were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5426

**Message:** Partial success - one or more of the requested pluggable databases did not contain any of the requested data files.

**Explanation:** The backup request for the database was for specific lists of pluggable databases and data files. These lists were verified in the database and one or more of the requested pluggable databases did not contain any of the requested data files. The data files that were found in the pluggable databases were backed up.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information. Confirm the list of data files that are specified in the Oracle Intelligent Policy are correct and in the requested pluggable databases. Update the lists, where applicable, in policy. If the pluggable databases or data files were specified using the command line, please confirm their spelling. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5427

**Message:** Partial success - more than one error was encountered, please refer to the **Detailed Status** tab in the **Job Details** and review logs for more information.

**Explanation:** Multiple errors were encountered while the request was processed. Some items were successfully processed. The database objects (pluggable database, tablespace, and data files) that were successful are contained in the backup.

**Recommended Action:** Check the detailed status of the associated jobs in the activity monitor for more information on the errors. Depending on the errors, make the appropriate changes to the policy. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5428

**Message:** No database backup shares were found.

**Explanation:** No database backup shares were found during backup.

**Recommended Action:** Configure the appliance database backup share and then backup the files to the share using the database vendor's tools. NetBackup does not retry this job after failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5429

**Message:** No new files or files that are related to the instance or database were found in the database backup share.

**Explanation:** No new files or files that are related to the instance or databases (configured in the OIP) found in the database backup share.

**Recommended Action:** Make sure that a backup is on the database backup share before the policy is executed. If the policy contained an incremental schedule, then verify that the database backup share contained new files. NetBackup does not retry this job after failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5430

**Message:** Database must be in `ARCHIVELOG` mode to perform a cold backup of a pluggable database.

**Explanation:** A cold backup of a pluggable database was requested. This configuration is not an Oracle supported environment. The database must be in `ARCHIVELOG` mode to perform a cold backup of a pluggable database.

**Recommended Action:** Change the database to `ARCHIVELOG` mode or change the backup request from a cold backup to a hot backup. Retry the backup once the updates are complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5431

**Message:** The requested operation did not get a response from the NetBackup appliance.

**Explanation:** The requested operation did not get a response from the NetBackup appliance within the configured timeout.

**Recommended Action:** The default timeout is set to 60 seconds. Configure a new timeout on the NetBackup master server. After the timeout is configured on the master server, confirm the NetBackup appliance is active and retry the operation.

- On Windows: Add a registry `DWORD` entry that is called `APPLIANCE_TIMEOUT` with a value in seconds at  
`HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config`
- On UNIX: Change the `APPLIANCE_TIMEOUT` setting in the `bp.conf` file

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5432

**Message:** The requested NetBackup appliance operation is unsuccessful.

**Explanation:** NetBackup sent a request to the NetBackup appliance and the requested operation did not complete successfully.

**Recommended Action:** Review the NetBackup appliance error message log, the *NetBackup Appliance Troubleshooting Guide*, or contact the NetBackup appliance administrator for help.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5433

**Message:** The NetBackup request did not complete due to a NetBackup appliance communication issue.

**Explanation:** NetBackup cannot communicate with the NetBackup appliance. This issue can be due to network issues or the NetBackup appliance is not online.

**Recommended Action:** Review the NetBackup appliance error message log, the *NetBackup Appliance Troubleshooting Guide*, or contact the NetBackup appliance administrator for help.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5434

**Message:** Cannot validate the identity of the NetBackup appliance.

**Explanation:** NetBackup cannot validate the identity of the NetBackup appliance.

**Recommended Action:** Review the NetBackup appliance error message log, the *NetBackup Appliance Troubleshooting Guide*, or contact the NetBackup appliance administrator for help.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5435

**Message:** Recovery point operations (`-create`, `-delete`, or `-list`) must be initiated from a master server.

**Explanation:** A NetBackup client does not have permission to use this `nborair -create`, `-delete`, or `-list` command options. These options are run from the master server using root user (UNIX) or administrator (Windows) access.

**Recommended Action:** Contact the NetBackup administrator to run the `nborair -create`, `-delete`, or `-list` command options from the master server. The NetBackup administrator must have root user (UNIX) or administrator (Windows) access on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5436

**Message:** No recovery point was found.

**Explanation:** No recovery points were found on the selected NetBackup appliance.

**Recommended Action:** Confirm there is a recovery point created. If there is no recovery point, create a recovery point and retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5437

**Message:** Partial success - recovery points from one or more database shares were not found.

**Explanation:** NetBackup was unsuccessful in finding recovery points for one or more database shares.

**Recommended Action:** Review the NetBackup debug logs (`bprd`, `nboair`) for more details about the error. Also, review the NetBackup appliance debug logs for further details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5438

**Message:** The requested export path information is not found.

**Explanation:** NetBackup was unsuccessful finding information about the requested export path.

**Recommended Action:** List all recovery points and see if the requested export path `/recovery` point is available. Review the NetBackup debug logs (`bprd`, `nboair`) for more details about the error. Also, review the NetBackup appliance debug logs for further details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5439

**Message:** Validation unsuccessful. The recovery point was not created from the specified backup ID.

**Explanation:** The recovery point mounted at the specified path was not created from the specified backup ID.

**Recommended Action:** Confirm that you requested the correct mount path. Also, confirm that you have requested the correct backup ID in the create recovery point process. Check with the NetBackup administrator for the correct backup ID in the create recovery point process and system administrator for the correct export mount path.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5440

**Message:** Required environment variable is not set.

**Explanation:** For the validate operation on Windows, the environment variable `ORACLE_HOME` is required to be set.

**Recommended Action:** You need to set the required environment variable `ORACLE_HOME` with the appropriate value and perform the validate operation again. Review the NetBackup debug logs (`nborair`) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5441

**Message:** Attempt to open Oracle direct NFS file was unsuccessful.

**Explanation:** NetBackup attempted to open Oracle direct NFS file and was unsuccessful.

**Recommended Action:** When NetBackup performs the validate operation on Windows, we get the mount path that is associated with the set export path from Oracle direct NFS file. Confirm that the correct value is set in the environment variable `ORACLE_HOME`. Review the NetBackup debug logs (`nborair`) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5442

**Message:** Attempt to retrieve the device information from the NFS mount path was unsuccessful.

**Explanation:** The attempt to retrieve the NFS server and export path details was unsuccessful.

**Recommended Action:** Confirm that the provided mount path is correct and that the path is rightly mounted (UNIX) or Oracle direct NFS file (Windows) has the correct entries. Review the NetBackup debug logs (`nborair`) for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5443

**Message:** Backup ID cannot be used for Oracle instant recovery.

**Explanation:** The specified backup ID does not contain a snapshot that can be used for instant recovery.

**Recommended Action:** Use the `nborair` command with `-list_images` option to view which images should be used for instant recovery and specify a different backup ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5444

**Message:** The NetBackup appliance credentials retrieval was unsuccessful.

**Explanation:** NetBackup cannot find the credentials of the NetBackup appliance.

**Recommended Action:** Review the NetBackup appliance error message log, the *NetBackup Appliance Troubleshooting Guide*, or contact the NetBackup appliance administrator for help.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5445

**Message:** Oracle instant recovery share cannot be used for backup operations.

**Explanation:** Copilot instant recovery shares cannot not be used for backup operations.

**Recommended Action:** A Copilot instant recovery share cannot be used in a backup policy.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5446

**Message:** Partial success - backup of one or more of the requested shares unsuccessful.

**Explanation:** NetBackup was unsuccessful in backing up one or more shares due to failure or an unsupported configuration.

**Recommended Action:** Review the detailed status of the backup job and the `bpdbsbora` debug logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5447

**Message:** Could not resolve appliance host name from IP address.

**Explanation:** The appliance is configured in NetBackup with its IP address.

**Recommended Action:** Update the NetBackup server list or media server list to use the appliance host name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 5448

**Message:** Could not match the appliance to a server in the client's server list.

**Explanation:** The appliance IP address did not match any entries in the client's server list.

**Recommended Action:** Add the appliance host name to the client's server list.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5449

**Message:** The script is not approved for execution.

**Explanation:** The script that is listed in the policy was not in the default location or any authorized location.

**Recommended Action:** Move the script to the default location or add the path as an authorized location using the `nbsetconfig` or `bpsetconfig` command. The default location for UNIX is: `/usr/openv/netbackup/ext/db_ext`. The default location for Windows is: `install_path\netbackup\dbext`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5450

**Message:** No scripts or paths are approved for execution on this client.

**Explanation:** `DB_SCRIPT_PATH=none` was set on this client to prevent scripts from executing.

**Recommended Action:** Consult the client administrator for information as to why `none` was set on this client.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5451

**Message:** The script is stored in a remote location.

**Explanation:** The script exists in a remote network location and cannot be executed.

**Recommended Action:** Move the script to a local authorized location for execution.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5452

**Message:** The script cannot be accessed for execution.

**Explanation:** The script either does not exist or is not accessible by the NetBackup client service.

**Recommended Action:** Confirm that the script and its location are on the local system and NetBackup can access the script. For Windows clients, be sure to verify that the user running the NetBackup client service has `read` and `execute` permissions for the script.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5500

**Message:** The NetBackup core web service service internal error

**Explanation:** An internal error occurred in the NetBackup core web service.

**Recommended Action:** Submit a problem report and provide the appropriate logs and the request that caused the error. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5501

**Message:** Supplied URI is too short

**Explanation:** The URL in the HTTP request is incomplete and does not have the components required for the request.

**Recommended Action:** Check the URL that is supplied in the HTTP request and correct if necessary. Resubmit the request. If the problem persists, submit a problem report and provide the appropriate logs and the URL for the request. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5502

**Message:** Supplied URI is not supported

**Explanation:** The core web service receives a request for an unsupported URL.

**Recommended Action:** Check the list of supported uniform resource identifiers (URIs) by the core web service and retry with a supported URI. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5503

**Message:** NetBackup core web service is terminating

**Explanation:** The NetBackup Service Layer (NBSL) service is in the process of shutting down when it receives the HTTP request.

**Recommended Action:** Ensure that the NetBackup core web service is enabled. Restart NBSL and retry the request. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5504

**Message:** Query string in URI is bad

**Explanation:** The query string in the received HTTP request is bad.

**Recommended Action:** Correct the query string in the request then retry the request. If the problem persists, submit a problem report with the appropriate logs and the URL of the request. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5505

**Message:** Client name is required

**Explanation:** The core web service receives a `vmimagelist` request with the client name that is not supplied in the query filter.

**Recommended Action:** Include the correct client name in the `vmimagelist` request, then retry the request. If the problem persists, submit a problem report with the appropriate logs and the URL of the request. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5506

**Message:** Failed to communicate with core web service proxy

**Explanation:** The core web service is unable to communicate with `nbproxy` to process the incoming request.

**Recommended Action:** Restart NBSL, then retry the request. If the problem persists, submit a problem report with the appropriate logs and the URL of the request. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5507

**Message:** Unknown jobid

**Explanation:** The core web service receives a request for job details (for example `/job/<jobid>`), but NetBackup does not recognize the supplied `jobid`.

**Recommended Action:** Retry the request with a `jobid` that NetBackup recognizes and has not yet been deleted.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5508

**Message:** Error in parsing XML document

**Explanation:** The core web service is unable to parse the XML response document that `bprd` sent in response to the restore precheck request.

**Recommended Action:** Check the arguments that are passed to the restore pre-check request, then retry the request. If the problem persists, submit a problem report with the appropriate logs and the request details. The NetBackup core web service sends log messages to the NBSL log (OID=443).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5626

**Message:** After you upgrade both the source and the target master server, you must update the trust relationship on both of the servers. After you update the trust

relationship, you can make configuration changes related to the trusted master servers.

**Explanation:** The trust relationship implementation for remote master servers has been changed for targeted Auto Image Replication (A.I.R.) on version 8.1 and later. After you upgrade both the source and the target master servers from a pre-8.1 version to a version that is 8.1 or later, you must update the trust relationship between both of the master servers. If you do not update the trust, you cannot create or modify any storage lifecycle policies on the source master server.

**Recommended Action:** Run one of the following commands on both the source and the target master server.

Run the following command if you are using user credentials; you are prompted to provide the password:

```
nbseccmd -setuptrustedmaster -update -masterserver
master_server_name -remotemasterserver remote_master_server
-domainname domain_name -username username -fpfile filename
```

Run the following command if you are using an authorization token; you are prompted to provide the token:

```
nbseccmd -setuptrustedmaster -update -masterserver
master_server_name -remotemasterserver remote_master_server
-domainname domain_name -fpfile filename
```

Run the following command if you are using the answer file:

```
nbseccmd -setuptrustedmaster -update -info answer_file
```

For more information about the `nbseccmd` command, see the [NetBackup Commands Reference Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5761

**Message:** Failed to initialize Windows Socket library

**Explanation:** On Windows, NetBackup encountered an error initializing the Microsoft Windows socket communication library.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5762

**Message:** Peer is not a NetBackup Master or Media Server

**Explanation:** A NetBackup host returns this code if it does not recognize the NetBackup server.

**Recommended Action:** Verify that the requesting NetBackup server is indeed the master server as recognized by the NetBackup host returning this status code.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5763

**Message:** Encountered error during socket communication

**Explanation:** A Logging Assistant process encounters a socket communication problem while operating on the master server or the NetBackup host.

**Recommended Action:** If NetBackup is otherwise functioning correctly, this error requires Veritas Support assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5764

**Message:** Command specified for execution is invalid or not allowed

**Explanation:** A Logging Assistant process encounters this error on a NetBackup host.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5765

**Message:** Failed to execute specified command (CreateProcess or exec)

**Explanation:** A Logging Assistant process encounters this error on a NetBackup host while it performs the requested action. This error may indicate problems with system resources or even a product defect.

**Recommended Action:** Retry the Logging Assistant action. If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5766

**Message:** Failed to execute specified command (fork)

**Explanation:** A Logging Assistant process encounters this error on a NetBackup host while it performs the requested action. This error may indicate problems with system resources on the host.

**Recommended Action:** Retry the Logging Assistant action. If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5767

**Message:** Failed to get exit code of child process

**Explanation:** A Logging Assistant process encounters this error on a NetBackup host on a failure to get the exit status of a child process while it performs a requested action. One possible cause for this error can be manual intervention.

**Recommended Action:** If this error is not the result of manual intervention, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5768

**Message:** Failed to read complete output of executed command

**Explanation:** Socket connection problems exist between the Logging Assistant processes on master server and the NetBackup host.

**Recommended Action:** Retry the Logging Assistant action. If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5769

**Message:** Failed to reap exit code of child process

**Explanation:** Returned by a Logging Assistant process on UNIX/Linux NetBackup host on failure to get exit status of the child process while performing requested action. One possible cause for this error can be manual intervention.

**Recommended Action:** If this error is not the result of manual intervention, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5770

**Message:** Failed to get cluster configuration

**Explanation:** This status code should not be encountered.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5771

**Message:** Failed to write output received from remote command

**Explanation:** Socket connection problems exist between the Logging Assistant processes on the master server.

**Recommended Action:** If this error is not the result of manual intervention, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5772

**Message:** Failed to read unified logging configuration file

**Explanation:** A VxUL configuration file is missing or malformed.

**Recommended Action:** Check the existence and the format of the VxUL configuration file that was mentioned along with the error message on the specified NetBackup host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 5773

**Message:** Failed to get virtual name of Master Server

**Explanation:** This status code should not be encountered.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5774

**Message:** Specified logs are not valid

**Explanation:** A product may be defective.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5775

**Message:** Invalid option specified

**Explanation:** A product may be defective.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5776

**Message:** Failed to spawn new process

**Explanation:** A product may be defective.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5777

**Message:** Failed to create the staging directory on Master Server

**Explanation:** Logging Assistant failed to create the specified staging directory on the master server.

**Recommended Action:** Verify that the specified path already exists. If not, try to create it manually.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5778

**Message:** Failed to read Logging Assistant database

**Explanation:** Logging Assistant is unable to read database file path and file contents.

**Recommended Action:** Check permissions of the Logging Assistant database file:

UNIX: /usr/opensv/var/global/logasst.db

Windows: <Install Path>\Veritas\NetBackup\var\global\logasst.db

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5779

**Message:** Failed to lock Logging Assistant database

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5780

**Message:** Failed to set non-inherit flag on database file handle

**Explanation:** This error can occur only on Windows.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5781

**Message:** Failed to prepare to save Logging Assistant database

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5782

**Message:** Failed to start to write Logging Assistant database

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5783

**Message:** Failed to save Logging Assistant database

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5784

**Message:** Failed to access or write the readme or progress file

**Explanation:** The parent directory from which to read or in which to write the README or Progress file is missing or has incorrect permissions.

**Recommended Action:** Please check the specified path.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5786

**Message:** Logging Assistant record does not exist

**Explanation:** Another GUI instance has deleted the Logging Assistant record.

**Recommended Action:** Refresh the Logging Assistant GUI, then check if the record has been deleted.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5787

**Message:** Logging Assistant record already exists

**Explanation:** None

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5788

**Message:** Debug logging has not been set up for Logging Assistant record

**Explanation:** The Logging Assistant GUI is out of sync.

**Recommended Action:** Refresh the Logging Assistant GUI view and retry.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5789

**Message:** Failed to interpret `bpdjobs` output for job detail

**Explanation:** The Logging Assistant encountered interpreting information fetched from the Jobs database. The Logging Assistant cannot make pre-selections for debug logging to set up based on the Job database.

**Recommended Action:** Manually select the debug logging to set up. Contact Veritas Technical Support to investigate the Job Analysis failure.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5790

**Message:** Failed to fetch PureDisk configuration setting from Windows registry

**Explanation:** NetBackup cannot read the PureDisk configuration information.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5794

**Message:** Failed to calculate debug logs size for preview

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5796

**Message:** Logging Assistant agent encountered failure writing on socket to Master Server

**Explanation:** A socket connection problem exists between Logging Assistant processes on the master server and the NetBackup host.

**Recommended Action:** Retry the Logging Assistant action. If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5798

**Message:** Failed to list disk volumes on Master Server using `bpmount`

**Explanation:** This error occurs when the Logging Assistant enumerates partitions on Windows while fetching free disk space information.

**Recommended Action:** If the error persists, contact Veritas Technical Support. You may still be able to manually establish free space information and initiate the intended action such as log collection.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5799

**Message:** Failed to get disk space information of volumes or mount points

**Explanation:** Logging Assistant tries to fetch free disk space information.

**Recommended Action:** If the error persists, contact Veritas Technical Support. You may still be able to manually establish free space information and initiate the intended action such as log collection.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5800

**Message:** Failed to execute `bpdjobs` to fetch job details

**Explanation:** Logging Assistant may be defective.

**Recommended Action:** If the error persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5801

**Message:** Failed to fetch job details. Check if job exists.

**Explanation:** The specified Job ID for Job Analysis that suggests what debug logging to set up does not exist in the Jobs database.

**Recommended Action:** If the specified job ID does exist, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5803

**Message:** Failed to modify PureDisk configuration file

**Explanation:** None

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5804

**Message:** Failed to modify Java GUI configuration file (`Debug.properties`)

**Explanation:** None

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5805

**Message:** Remote host NetBackup version not supported by the Logging Assistant

**Explanation:** The Logging Assistant supports setting up debug logging on (and collecting debug logs from) hosts that run NetBackup version 7.7 or higher.

**Recommended Action:** None

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5806

**Message:** Unexpected contents of PureDisk configuration file (`pdregistry.cfg`)

**Explanation:** None

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5807

**Message:** Failed to copy `nbcplogs/nbsu` output file from remote host

**Explanation:** The Logging Assistant contacts `bpcd` to copy the `nbcplogs` and `nbsu` output files from the NetBackup host.

**Recommended Action:** Check that the connection from the master server to `bpcd` can be set up by using `bptestbpcd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5808

**Message:** Failed to load PBX configuration to change log level

**Explanation:** A PBX configuration file may be missing or malformed.

**Recommended Action:** Check the existence and format of the PBX configuration file and the error message on the specified NetBackup host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5809

**Message:** Invalid PBX Debug Log Level specified

**Explanation:** The PBX logging level is invalid.

**Recommended Action:** Set the PBX logging level to an appropriate value.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5811

**Message:** Temporary directory to use for logs collection does not exist

**Explanation:** The Logging Assistant failed to create the temporary directory on a NetBackup host in which to collect the `nbcpllogs` or `nbsu` output.

**Recommended Action:** Check the directory permissions on the NetBackup host. Also verify that the parent directory of the specified temporary directory exists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5812

**Message:** `nbcpllogs` exited with error

**Explanation:** This status code should not be encountered.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5813

**Message:** `nbcpllogs` did not collect any logs

**Explanation:** None

**Recommended Action:** Check that the debug logs on the host are available to collect. If the debug logs relevant to the Logging Assistant record exist on the host, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5814

**Message:** `nbsu` exited with error

**Explanation:** None

**Recommended Action:** Contact Veritas Technical Support.



Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5815

**Message:** No activity for the Logging Assistant record is in progress

**Explanation:** The Logging Assistant GUI is out of sync.

**Recommended Action:** Refresh the Logging Assistant GUI and retry.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5816

**Message:** Collect debug logs operation canceled

**Explanation:** Not available.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5817

**Message:** Collect nbsu operation canceled

**Explanation:** Not available.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5819

**Message:** Cancel operation requested

**Explanation:** Not available.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5820

**Message:** Not a valid Logging Assistant temporary directory for clean-up

**Explanation:** Not available.

**Recommended Action:** Not available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5821

**Message:** Failed to get policy details

**Explanation:** To suggest debug logging to set up, the Logging Assistant fetches policy information that is associated with the job ID submitted for analysis. However, the policy does not exist.

**Recommended Action:** If the associated policy does exist, please contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5902

**Message:** Fingerprint of the certificate could not be generated.

**Explanation:** The CA certificate may not be in the trust store.

**Recommended Action:** Run the `nbcertcmd -getCACertificate` command and try to generate the CA certificate again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5903

**Message:** CA certificate could not be verified.

**Explanation:** The CA certificate that is on the host cannot be used to perform the request. Trust is not established with the NetBackup host to which you are trying to communicate. The CA certificate is not in the trust store in the host certificate database or the trust store has more than one certificate with the same name (usually, a generic name like `localhost.localdomain`). The web service certificate may also have expired.

**Recommended Action:** The NetBackup host must trust the CA. Check if the CA certificate was added to the trust store with the `nbcertcmd -listCACertDetails` command. Run the `nbcertcmd -getCACertificate` command to add the certificate to the trust store.

If the trust store has multiple certificates with the same (generic) name, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5904

**Message:** Internal error.

**Explanation:** One of the internal services has failed to respond.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5905

**Message:** The host ID is not valid.

**Explanation:** The master server does not recognize the specified host ID.

**Recommended Action:** Check the specified host ID using the `nbcertcmd -listCertDetails` command. If the specified NetBackup host is part of multiple NetBackup domains, ensure that you are providing the correct host ID that corresponds to the specified NetBackup domain.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5906

**Message:** The token is not valid.

**Explanation:** The generated token is not valid.

**Recommended Action:** Redo the action. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5907

**Message:** Unknown resource requested.

**Explanation:** The certificate that you are trying to view or to execute related operations does not exist.

**Recommended Action:** Verify the certificate details that you provided. Details can include a serial number, host ID, or host name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5908

**Message:** Unknown error occurred.

**Explanation:** The certificate generation, renewal, or retrieval operation failed.

**Recommended Action:** Save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5909

**Message:** Token does not exist for this token value.

**Explanation:** The token value that you provided is not correct.

**Recommended Action:** Provide the correct token value and rerun the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5910

**Message:** Host name is not specified.

**Explanation:** The operation failed to retrieve the required information.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5913

**Message:** A token with this name already exists.

**Explanation:** The token name that you are using to create the new token already exists.

**Recommended Action:** Provide a new name and then recreate the token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5914

**Message:** The security service is not available.

**Explanation:** The NetBackup web service is not reachable or is not running on the master server.

**Recommended Action:** Check the network connectivity of the host on which you are performing the operation. Contact the NetBackup administrator to correct the status of the NetBackup web service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5915

**Message:** Request timed out.

**Explanation:** A request to the NetBackup web service has failed due to a network timeout.

**Recommended Action:** Check the network connectivity of the host on which you are performing the operation. Contact the NetBackup administrator to correct the status of the NetBackup web service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5916

**Message:** Token name is not specified.

**Explanation:** The operation failed to retrieve the token information from the request because the token name was not specified by the user in the request.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5917

**Message:** The reissue token cannot have the usage count greater than one.

**Explanation:** The re-issue token cannot be a multi-use token.

**Recommended Action:** A multi-use token cannot be associated with the host. The re-issue token cannot be a multi-use token. Take appropriate action and generate the required token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5918

**Message:** The maximum usage count for the token should be provided within the valid range, which is from 1 to 99999.

**Explanation:** A token can be used from 1 to 99,999 times. The maximum usage count that you selected has exceeded the allowable usage count.

**Recommended Action:** Select a valid usage count.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5919

**Message:** Validity period specified for this token is not valid. The maximum validity period that you can specify is 999 days.

**Explanation:** A token can have a validity period from 1 – 999 days. The validity period specified exceeded the allowable validity period.

**Recommended Action:** Select a valid period.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5920

**Message:** The specified token is associated with a different host name.

**Explanation:** The specified token is not associated with the requesting host.

**Recommended Action:** Verify that you are using the correct token. If the specified NetBackup host is associated with multiple NetBackup domains, ensure that you are using the token that corresponds to the appropriate NetBackup domain.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5921

**Message:** The specified token is associated with a different host ID.

**Explanation:** The specified token is not associated with the host.

**Recommended Action:** Verify that you are using the correct token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5922

**Message:** The reissue token cannot be associated with the host name.

**Explanation:** You cannot generate a token using both the host ID and the host name.

**Recommended Action:** Use either the host ID or the host name and try to regenerate the token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5925

**Message:** The required data is missing.

**Explanation:** Certificate generation or renewal is requested, but the Certificate Signing Request (CSR) file sent with the request is empty.

**Recommended Action:** Ensure that all of the required inputs provided are correct and retry the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5926

**Message:** Certificate signing request is not valid.

**Explanation:** The certificate that signed the request file is not in the expected format.

**Recommended Action:** Regenerate the certificate request file, rerun the operation, and ensure that the data has not changed in transit.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5927

**Message:** The specified file could not be opened.

**Explanation:** The specified file might not exist or you do not have permission to access the file.

**Recommended Action:** Use a valid file name and try to open the file or check permissions.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5929

**Message:** The certificate is not in the Active state, so it cannot be renewed.

**Explanation:** A certificate has three states: active, revoked, and expired. You cannot renew revoked certificates.

**Recommended Action:** Send the certificate re-issue request after performing corrective actions. If you want to use the same credential (key pair), then the new certificate can be generated using the re-issue token. You can use the following command:

```
nbcertcmd -getCertificate
```

If you plan to change credentials, see the [NetBackup Security and Encryption Guide](#) for workflow details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5930

**Message:** The request could not be authorized.

**Explanation:** The master server is unable to validate the client certificate. Possible causes for this are as follows:

- The client certificate has expired. You can run the `nbcertcmd -getCertDetails` or `nbcertcmd -getCertDetails -cluster` command to confirm.
- The client key pair has changed and the host has obtained (or renewed) a certificate from another master server.
- The certificate for the host has been revoked.
- A web authentication token is required for a NetBackup web application operation (`nbcertcmd`). You will see this error if the user has not been authenticated.



**Recommended Action:** Use a re-issue token with the `nbcertcmd -getCertificate` command. If the user has not been authenticated, use the `bpbnt -login -logintype WEB` command to get a web authentication token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5931

**Message:** The host ID is empty.

**Explanation:** The host ID cannot be found in the revoke certificate request.

**Recommended Action:** Resend the request. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5932

**Message:** Token usage count is not set.

**Explanation:** An attempt to generate an authorization token with a zero usage count was performed.

**Recommended Action:** Generate a token with valid parameters. The allowable count is from 1 to 99,999.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5933

**Message:** The maximum token usage limit has been reached.

**Explanation:** An authorization token has a fixed usage count. If the usage count exceeds the allowable usage count, the token cannot be used.

**Recommended Action:** Create a new token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5934

**Message:** The token has expired.

**Explanation:** The token validity period has reached the maximum limit and has expired. This token can no longer be used.

**Recommended Action:** Create a new token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5936

**Message:** The specified token name is not in a valid format.

**Explanation:** The name specified for the token contains invalid characters.

**Recommended Action:** Specify a valid token name. The valid characters are A-Z, a-z, 0-9, and \_.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5938

**Message:** The revocation reason code is not valid.

**Explanation:** NetBackup supports only revocation reason codes from 1 to 5.

**Recommended Action:** Specify a valid reason code and then try to revoke the certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5939

**Message:** This revocation reason code is not supported by the server.

**Explanation:** NetBackup supports only revocation reason codes from 1 to 5.

**Recommended Action:** Specify a valid reason code and then try to revoke the certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5940

**Message:** Reissue token is mandatory; please provide a reissue token.

**Explanation:** A certificate reissue requires a reissue token that is associated with a specific host ID.

**Recommended Action:** Generate a reissue token for the required host and then request a certificate reissue. Use the following command (or the **NetBackup Administration Console**) to generate the reissue token:

```
nbcertcmd -createToken -name name_of_token -reissue  
[-host host_name | -hostId host_id]
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5941

**Message:** The host ID is not associated with any host.

**Explanation:** The specified host ID is not known to the master server.

**Recommended Action:** Verify that the specified host ID corresponds to the specified master server. Use the `nbcertcmd -listCertDetails` command on the specified NetBackup host to find the host ID that corresponds to the specified master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5942

**Message:** Certificate could not be read from the local certificate store.

**Explanation:** The certificate was not added to the local certificate store or it may be lost or corrupted. You may also have no administrator privileges on the given NetBackup host.

**Recommended Action:** Check if you have administrator privileges on the specified NetBackup host. If you have the required privileges, use the `-force` option with the `nbcertcmd -getCertificate` command to regenerate the existing certificate. You may have to supply a token with this command, depending on the certificate deployment security levels specified on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5943

**Message:** Lock cannot be acquired on the file for writing.

**Explanation:** There was an error updating the file.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5944

**Message:** The host alias list has multiple host names.

**Explanation:** The certificate signing request contains multiple host names and only a single host name is supported.

**Recommended Action:** Specify a single host name in the certificate signing request and resend the request to the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5945

**Message:** Host alias is not specified.

**Explanation:** The certificate signing request does not contain a host name.

**Recommended Action:** Specify a host name in the certificate signing request and resend the request to the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5946

**Message:** Token is mandatory; please provide a token.

**Explanation:** The certificate deployment security level on the master server does not support the auto deployment of the certificate for the given host.

**Recommended Action:** Generate an authorization token and then run the `nbcertcmd -getCertificate` command to request a certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5947

**Message:** The host is not registered with the server.

**Explanation:** The specified host could not be found.

**Recommended Action:** Specify the correct host name or use a valid authorization token and rerun the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5948

**Message:** Certificate could not be written to the local certificate store.

**Explanation:** You might not have administrator privileges on the specified NetBackup host to add the certificate to the local certificate store.

**Recommended Action:** Check if you have administrator privileges on the given NetBackup host. If you have the required privileges, redo the action. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5949

**Message:** Certificate does not exist.

**Explanation:** A certificate from the specified server does not exist on the NetBackup host.

**Recommended Action:** Ensure that the appropriate certificate is deployed. See the [NetBackup Security and Encryption Guide](#) for details on how to deploy certificates.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5950

**Message:** Certificate already exists.

**Explanation:** A certificate from the specified server already exists on the requesting NetBackup host.

**Recommended Action:** Use the `nbcertcmd -getCertificate -force` command to overwrite the existing certificate, if required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5953

**Message:** The certificate deployment level is not valid.

**Explanation:** The certificate deployment level that you are trying to set is invalid.

**Recommended Action:** Select a certificate deployment level between 0 - 2 and rerun the command to set the certificate deployment level. For more information on certificate deployment levels, see the [NetBackup Security and Encryption Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5954

**Message:** The host name could not be resolved to the requesting host's IP address.

**Explanation:** The master server is unable to resolve the host name to the peer IP address of the NetBackup host that is requesting the certificate.

**Recommended Action:** Verify and correct your network configurations so that the master server can resolve the host name to the peer IP address. Alternatively, you can use an authorization token to deploy the certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5955

**Message:** The host name is not known to the master server.

**Explanation:** The host name is not on the known hosts list.

**Recommended Action:** Ensure that the host entry exists on one of the following locations: the server configuration list, the EMM database, at least 1 catalog image (not more than 6 months old), the clients listed in policies, or the client DB entry. Alternatively, you can use an authorization token to deploy the certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5956

**Message:** The existing certificate deployment level on the master server does not allow this operation.

**Explanation:** The certificate deployment security level set for the host does not let you deploy the host ID-based security certificate or add the CA certificate to the trust store without verification.

**Recommended Action:** If you see this error message while you are retrieving the host ID-based certificate, ensure that you use a valid authorization token with the `-getCertificate` option.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5957

**Message:** The master server is unable to connect to the CA.

**Explanation:** The master server is unable to connect to the NetBackup AT broker.

**Recommended Action:** Check the status of the NetBackup AT broker on the master server. Restart the service, if required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5958

**Message:** The master server is unable to access the CA certificate.

**Explanation:** The Web service user on the master server does not have the required permissions to access the CA certificate.

**Recommended Action:** Ensure that the web service user has the required permissions to read the CA certificate on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5959

**Message:** The NetBackup AT credentials of the web service user are not valid.

**Explanation:** The web service users' AT credentials are invalid or have expired.

**Recommended Action:** Stop the web service on the master server, run the `nbcertconfig -u -user webservice_user` command, and restart the web service.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5960

**Message:** NetBackup AT configuration on the master server could not be initialized.

**Explanation:** The AT configuration initialization failed or the web service user does not have the required permissions to access its certificate store.

**Recommended Action:** Ensure that the web service user has the required permissions to access the certificate store on the master server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5962

**Message:** The host name does not match the existing name in the certificate.

**Explanation:** The host ID certificate renewal is attempted for the host whose host name is changed.

**Recommended Action:** If the NetBackup host administrator wants to get the certificate for the given host with the new name, then perform the following steps:

1. The NetBackup host administrator should ask the NetBackup administrator to revoke the certificate of the host by using the `-host host_name | -hostId host_id` options. The NetBackup administrator can use the following command:

```
nbcertcmd -revokeCertificate -reasonCode value
-host old_host_name | -hostId host_id
```

2. The NetBackup host administrator should ask the NetBackup administrator to generate a reissue token for a specific host. The NetBackup administrator can use the following command:

```
nbcertcmd -createToken -name token_name -reissue
-host old_host_name | -hostId host_id
```

3. After the NetBackup host administrator receives the reissue token, the following command can be used (specify the received token when prompted):

```
nbcertcmd -getCertificate -token -force
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5963

**Message:** Entity does not exist.

**Explanation:** The user is referring to an entity that does not exist when using a specific command. The possible entities are either an authorization token or a host



ID-based certificate. The user may be referring to a token with the wrong token name or the user may be referring to a certificate with an incorrect serial number.

**Recommended Action:** Check that the argument values supplied in the command are correct.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5964

**Message:** Data conversion error.

**Explanation:** There was an internal error while processing data.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5965

**Message:** The host ID associated with this reissue token is assigned to another host. You need to revoke the existing certificate for the host ID before you can reuse the host ID for this host.

**Explanation:** The user specified the `nbcertcmd -getCertificate` command using a reissue token. The user is trying to reissue a host ID to a host with a host name that is different than the one registered with the server. When a host is going through a name change and wants to ensure that its identity is maintained in the NetBackup domain, the user should revoke the existing certificate with the existing host name.

**Recommended Action:** The user must revoke the current certificate with the existing host name and then use the reissue token to request a certificate using the new host name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5966

**Message:** The host has an active certificate. You need to revoke the certificate before you can disassociate the host from its host ID.

**Explanation:** The user is trying to decouple an existing host and it has active certificates. In this case, the server will reject the decouple request as only the hosts that have revoked certificates can be decoupled from their existing host IDs.

**Recommended Action:** The user must revoke the certificate for this host and only then mark it as decoupled from the associated host ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5967

**Message:** The file already exists.

**Explanation:** The user provided a specific file name to perform an operation, but the file already exists at the specified location.

**Recommended Action:** The user can rename/move/delete the existing file or submit a new file name.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5968

**Message:** The host information could not be retrieved while creating the certificate signing request.

**Explanation:** While creating a certificate signing request for a given host, specific information such as the host name, host aliases, and host key pair is retrieved from the host. The `nbcertcmd` command failed to retrieve this information.

**Recommended Action:** Try the following possible solutions:

- Retry the current operation.
- Retry the current operation by restarting the system.
- If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5969

**Message:** Response from the NetBackup Web Management Console service could not be parsed.

**Explanation:** The response received from the NetBackup web management console service while executing current operation is in an unknown or incorrect format.

**Recommended Action:** Retry the current operation. If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5970

**Message:** The server time could not be fetched.

**Explanation:** The current server time could not be retrieved.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5971

**Message:** The token contains characters that are not supported.

**Explanation:** The token value passed in the token file contains characters that are not supported. NetBackup only supports the following characters as part of the token value (A-Z, a-z, and 0-9).

**Recommended Action:** Check the token value passed in the token file and ensure that it contains valid characters (A-Z, a-z, and 0-9). Ensure that the file encoding format is ANSI.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5972

**Message:** The certificate could not be revoked. It was already revoked or expired.

**Explanation:** When revocation of the already revoked or expired certificate is tried, it will not allow the revocation.

**Recommended Action:** Specify the active certificate and then try to revoke the certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5973

**Message:** The token type is not valid.

**Explanation:** To create a token, a valid token type is required.

**Recommended Action:** Specify one of the following token types:

- 0 - Default token
- 1 - Reissue token

If you have not provided the token type, the default token type (0) is automatically selected.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5974

**Message:** The specified token requires a host ID.

**Explanation:** To create a reissue token, a corresponding host ID is required.

**Recommended Action:** Provide a host ID of the host for which you want to create a token.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5976

**Message:** The passphrase must contain a minimum of 8 and a maximum of 20 characters.

**Explanation:** The length of the specified passphrase is out of the allowed range.

**Recommended Action:** Specify a passphrase with a minimum of 8 and a maximum of 20 characters.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5977

**Message:** The existing passphrase and the new passphrase must be different.

**Explanation:** The specified passphrase is the same as the existing one.

**Recommended Action:** Specify a passphrase that is different than the existing one.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5978

**Message:** Failed to refresh the certificate revocation list (CRL) and security level.

**Explanation:** This error can be due to following reasons:

- **Recommended Action:** Failed to fetch the CRL via the HTTP request
- Failed to save the CRL on the disk
- Failed to fetch the security level via the HTTP request
- Failed to update the `certmapinfo.json` with CRL and security level information
- Failed to get the CRL because a client in the DMZ could not connect to the HTTP tunnel on the media server

**Recommended Action:** Do the following, as appropriate:

- On the master server, examine the unified logs on the NetBackup server for `nbwebservice` (OID 466 and 484).
- On the media server, examine the `pbx` (OID 103), `nbpxytnl` (OID 490), and `nbpxyhelper` (OID 486) logs. `pbx` is logged to the following directories:  
 Windows: `install_path\VxPBX\log`  
 UNIX: `/opt/VRTSspbx/log`
- Ensure that the following are online:
  - Master server
  - NetBackup web service (`nbwmc`)
  - NetBackup relational database (`NBDB`)
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5979

**Message:** The certificate revocation list (CRL) in the certificate is invalid.

**Explanation:** The error can be due to following reasons:

- **Explanation:** The host failed to get the CRL when it requested the certificate via the HTTP request.
- The CRL is empty or has an invalid format.

**Recommended Action:** Do the following, as appropriate:

- On the host where the error occurred, examine the legacy logs for `nbcertcmd`. Use these logs to help troubleshoot issues that appear in the web services.
- On the master server, examine the unified logs for `nbweb service` (OIDs 466 and 484).
- Restart the services on the master server. Then, retry the following command for the host to fetch the CRL:

```
./nbcertcmd -getCrl
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5980

**Message:** The security level in the certificate is invalid.

**Explanation:** The host failed to get the security level with the certificate via the HTTP request.

**Recommended Action:** Do the following, as appropriate:

- On the master server, examine the unified logs on the NetBackup server for `nbweb service` (OID 466 and 484).
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- Run the following command for the host to fetch the CRL and the security level:

```
./nbcertcmd -getCrl
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5982

**Message:** The certificate revocation list (CRL) is unavailable.

**Explanation:** This error can occur for the following reasons:

- (Scenario 1) The NetBackup web service has not yet generated a CRL. The NetBackup web service attempts to generate a new CRL on startup. If the CRL has not been generated it means one of two things: NetBackup is working to create it. Or, there was a problem generating the CRL.
- (Scenario 2) The host does not have a CRL cached for the current domain.

**Recommended Action:** Do the following, as appropriate:

For Scenario 1, do the following:

- Retry the command or operation.
- Verify that `nbatd` is running on the master server, then retry the operation.
- Restart the services on the master server, then retry the operation.
- On the master server, examine the unified logs on the NetBackup server for `nbservice` (all OIDs).
- On the master server and on the host where the error occurred, examine the unified logs for `nbatd` (OID 18).

For Scenario 2, do the following:

- Run the following command for the master server and then retry the operation:  
`./nbcertcmd -getCrl -server master server name`
- On all hosts involved in the communication, examine the unified logs for `nbpkyhelper` (OID 486).
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5983

**Message:** The host certificate is revoked.

**Explanation:** The host certificate is present in the certification revocation list (CRL) and is revoked.

**Recommended Action:** Do the following, as appropriate:

- On the host where the error occurred, examine the legacy logs on the NetBackup server for `nbcertcmd`.
- On all of the hosts involved in the communication, examine the unified logs for `nbpkyhelper` (OID 486).
- If the certificate was revoked in error, reissue a certificate for the host.
- If the certificate was revoked as intended, an attempted security breach may have occurred.
- Contact your Security Administrator.
- To reissue a certificate for the host, see the [NetBackup Security and Encryption Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5986

**Message:** The certificate request for the host was rejected because the host could not be validated as a master server.

**Explanation:** The master server-specific parameters were sent with the `nbcertcmd -getCertificate` command, but the certificate was requested for a non-master server host.

**Recommended Action:** Ensure that you do not send the master server-specific parameters when you deploy the certificate on a non-master server host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5987

**Message:** Cannot fetch the host ID of the NetBackup master server. The master server does not have the certificate.

**Explanation:** The master server does not have the certificate or the NetBackup Service Layer (NBSL) on the master server is down.

**Recommended Action:** Ensure that the following occurs:

- NBSL is running on the master server
- If NBSL is running on the master server, ensure that the host ID-based certificate is deployed on the master server
- If the host ID-based certificate is deployed and if you still see this error, refer to the **Resolving the master server host name change issue** procedure..

### Resolving the master server host name change issue

This error may occur if the master server host name is changed from a Fully Qualified Domain Name (FQDN) to a short name (or vice versa) in any of the following scenarios:

- NetBackup installation after a disaster
- Manual update in the NetBackup configuration file (`bp.conf` file on the UNIX or Windows registry).

In the following example, NetBackup is installed on a master server with a short name and the catalog backup is run. After a disaster, NetBackup is installed on the master server in a disaster recovery mode, but this time with FQDN. However, the identity of the master server (or disaster recovery package) is restored with the short name. This can cause failure when reissuing the client certificates,



automatically renewing the client certificates and deploying new certificates on clients.

To resolve this issue, use the following steps:

1. Log on to the master server.
2. Run following command:

UNIX:

```
/usr/opensv/netbackup/bin/nbcertcmd -ping
```

Windows:

```
install_path\NetBackup\bin\nbcertcmd -ping
```

- If the command is executed successfully, proceed to next step.
- If it fails with the exist status code 8509 (The specified server name was not found in the web service certificate), then carry out the steps that are provided in the following technote:

[https://www.veritas.com/support/en\\_US/article.000126751](https://www.veritas.com/support/en_US/article.000126751)

Proceed to the next step.

3. Stop and start the NetBackup Web Management Console service on the master server. Use following the NetBackup command:

UNIX:

```
/usr/opensv/netbackup/bin/nbwmc -terminate
```

```
/usr/opensv/netbackup/bin/nbwmc -start
```

Windows:

```
install_path\NetBackup\wmc\bin\nbwmc.exe -stop -srvname "NetBackup  
Web Management Console"
```

```
install_path\NetBackup\wmc\bin\nbwmc.exe -start -srvname  
"NetBackup Web Management Console"
```

4. Perform the user login on the master server. Use the following command:

```
install_path/netbackup/bin/bpnbat -login -loginType WEB
```

For example:

```
install_path\netbackup\bin\bpnbat -login -loginType WEB  
Authentication Broker [abc.example.com is default]:  
Authentication port [0 is default]:  
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd,  
ldap)[WINDOWS is default]:  
Domain [abc.example.com is default]:
```

```
Login Name [administrator is default]:
Password:
Operation completed successfully.
```

5. Note the value of the key `Client_Name` for the master server. For a clustered master server, note the value of the key `Cluster_Name`. This can be found at the following locations:

**UNIX:** `/usr/openv/netbackup/bp.conf`

**Windows:** `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config`

This value can either be the FQDN or the short name. For example, `abc.example.com`.

6. Note the host ID of the master server. You can obtain its value by using the following command:

```
install_path\netbackup\bin\NBCertCmd -listCertDetails
```

For a clustered master setup, use the following command:

```
install_path\netbackup\bin\NBCertCmd -listCertDetails -cluster
```

This command may return multiple records (if only one record is returned, select the host ID provided in that record).

- If the host name obtained in step 5 is FQDN, then pick the record where the “Issued By” entry matches its short name.
- If the host name obtained in step 5 is a short name, then pick the record where the “Issued By” entry matches its FQDN.

For example:

```
install_path\netbackup\bin\NBCertCmd -listCertDetails
```

```
Master Server : abc
Host ID : xxxxxx-4201-4c6a-xxxx-xxxxx
Issued By : /CN=broker/OU=root@abc/O=vx
Serial Number : 0x62e108c90000000c
Expiry Date : Aug 21 08:42:54 2018 GMT
SHA1 Fingerprint : 50:89:AE:66:12:9A:29:4A:66:E9:DB:71:37:
C7:EA:94:8C:C6:0C:A0
```

```
Master Server : xyz
Host ID : yyyyyy-4785-4252-yyyy-yyyyy
Issued By : /CN=broker/OU=root@xyz.master1.com/O=vx
```

```
Serial Number : 0x6ede87a70000000a
Expiry Date : Aug 21 09:52:13 2018 GMT
SHA1 Fingerprint : FE:08:C2:09:AC:5D:82:57:7A:96:5C:C1:4A:
E6:EC:CA:CC:99:09:D2
```

Operation completed successfully.

Here, 2 records are returned. For the first record, the issuer name provided in the “Issued By” field matches the short name of the client\_name obtained in step 5. Select the host ID that appears in the first record.

7. Add a host ID-to-host name mapping. Map the host ID of the master server that you have obtained in step 6 to the host name that you have obtained in step 5.

Use the following command:

```
install_path/netbackup/bin/admincmd/nbhostmgmt -a -i host_ID -hm
host_name
```

For example:

```
install_path/netbackup/bin/admincmd/nbhostmgmt -a -i
xxxxxx-4201-4c6a-xxxx-xxxxx -hm abc.example.com
```

abc.example.com is successfully mapped to xxxxxx-4201-4c6a-xxxx-xxxxx.

You can also add this host ID-to-host name mapping using the **NetBackup Administration Console**. Use the **Security Management > Host Management > Hosts** tab.

8. Renew the host ID-based certificate of the master server by using the following command:

```
install_path/netbackup/bin/nbcertcmd -renewCertificate
```

For a clustered master server, use the following command:

```
install_path\netbackup\bin\nbcertcmd -renewCertificate -cluster
```

9. Continue with the certificate deployment on a client (this can be either a reissue certificate, the automatic renewal of a certificate, or a new certificate deployment).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5988

**Message:** The host name is not part of the host ID-to-host name mapping list.

**Explanation:** The requesting host name is not mapped with the respective host ID.

**Recommended Action:** Map the host name to the associated host ID. In the **NetBackup Administration Console**, use the **Security Management > Host Management > Hosts** tab or the `nbhostmgmt` command to add mappings.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5989

**Message:** The reissue token is mandatory as a certificate was already issued to this host. Revoke the existing certificate if it is active and map this host name to the associated host ID.

**Explanation:** The host names that are used during the installation and re-installation are different; however, the host names are associated with same host ID. This can happen if the host name used earlier is a shortname and the one used now is in FQDN or vice versa. You need to identify the host record in the **NetBackup Administration Console**, using the **Security Management > Host Management > Hosts** tab or the `nbhostmgmt` command and use the host ID to generate the reissue token. You can also ensure that the client name of the host matches the one in the above listing.

**Recommended Action:** To deploy a certificate using this new name, you need to provide a reissue token for the existing host ID. For successful re-installation using the new host name, ensure the following:

- If the host has an active certificate, revoke it.
- The host names are mapped to the associated host ID. In the **NetBackup Administration Console**, use the **Security Management > Host Management > Hosts** tab or the `nbhostmgmt` command to add mappings.
- The client name for the host matches the primary host name associated with the issued host ID.

---

**Note:** If you want to deploy a certificate on a host with a host name that matches an existing host ID-to-host name mapping of another host, you must either delete the existing host ID-to-host name mapping and retry the operation or add a new host in the host database.

For more information on how to add a host, see the [NetBackup Security and Encryption Guide](#).

---

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5990

**Message:** The specified host ID-to-host name mapping is shared by multiple hosts and the auto reissue certificate parameter is set for two or more hosts.

**Explanation:** The auto reissue certificate parameter is set for multiple hosts that share the same host ID-to-host name mapping. In this case, NetBackup cannot determine the host where the certificate needs to be reissued. Therefore, the certificate cannot be deployed.

**Recommended Action:** In the case of shared mapping, ensure that the auto reissue certificate parameter is set only for the required host. You can reset the parameter for other hosts by running the following command:

```
nbhostmgmt -allowautoReissueCert -autoReissue 0
```

Alternatively, you can use the [NetBackup Administration Console](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5991

**Message:** The specified host either does not exist or the auto reissue certificate parameter is not set for the host.

**Explanation:** In order for NetBackup to reissue the certificate on the specified host, it should be a valid host and the auto reissue certificate parameter should be set for the host.

**Recommended Action:** Ensure that the specified host exists and that the auto reissue certificate parameter is set for the host. If the host to be recovered does not exist, initiate the Prepare to Restore workflow again for the host. To set the auto reissue certificate parameter for the host, run the following command:

```
nbhostmgmt -allowautoReissueCert -autoReissue 1
```

Alternatively, you can use the [NetBackup Administration Console](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5992

**Message:** The certificate request has failed as the host information cannot be updated.

**Explanation:** NetBackup cannot update the host information.

**Recommended Action:** Retry the operation. If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 5993

**Message:** The certificate is not valid for this host.

**Explanation:** The certificate to be deployed may not be associated with the host.

**Recommended Action:** Verify that the certificate is issued for the same host and retry the operation. If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6000

**Message:** The provided path is not whitelisted

**Explanation:** A NetBackup host displays this code if it is not allowed to access the provided path.

**Recommended Action:** Veritas recommends using the NetBackup default paths for progress logs or rename file options; for example, use the `user_ops` folder. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration. For more information on how to add a custom path, see "BPCD\_WHITELIST\_PATH option for NetBackup servers and clients" in the [NetBackup Administrator's Guide, Volume I](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6530

**Message:** Unable to start SharePoint web service on server

**Explanation:** The NetBackup SharePoint GRT web service, `Veritas.NetBackup.SPServiceHost.exe`, does not start on the front-end server.

**Recommended Action:** The SharePoint GRT web service, `Veritas.NetBackup.SPServiceHost.exe`, is deployed by default on the NetBackup clients and starts only during the restores of SharePoint 2016 backups. After the restore is completed, the web service is stopped.

Verify that SharePoint 2016 has been installed correctly on the front-end server. You can also try to manually start the service, `Veritas.NetBackup.SPServiceHost.exe`, from the command line. Verify that the service starts during the restore and stops after the restore is completed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6531

**Message:** Validation of operating system user/password failed for client

**Explanation:** The SharePoint credentials are missing or the NetBackup client service is not running with SharePoint administrator rights.

**Recommended Action:** Configure the SharePoint credentials on all of the nodes that are used to browse, backup, or restore.

See "Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint" in the [NetBackup for Microsoft SharePoint Server Administrator's Guide](#).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6600

**Message:** The BigData policy job failed. Check and verify that you have entered valid credentials and provided correct entries for the application server or the backup hosts.

**Explanation:** This error occurs when there is an issue with validating a BigData policy.

**Recommended Action:** Check and verify that you have entered the valid credentials, provided correct entries for the application server or the backup hosts, and resolved any network connectivity issues.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6601

**Message:** One or more of the input parameters or arguments are invalid.

**Explanation:** The input parameter or the argument can become invalid for the following reasons:

- An incorrect or no value is specified for the application server or the backup host.
- NetBackup could not reach the application server or the backup host.
- NetBackup could not find the object to complete the job.
- An appropriate plug-in is currently unavailable.

**Recommended Action:** Check and verify that you have entered valid credentials and provided the correct entries for the application server or the backup host. Ensure that the BigData framework libraries are correctly installed on the computer.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6602

**Message:** Insufficient memory or inadequate resources available to complete the job.

**Explanation:** This error occurs because of the following reasons:

- The memory allocation to the system is insufficient.
- The resources that are available to the system are inadequate.

**Recommended Action:** Ensure that sufficient memory is allocated and adequate resources are available to the system.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6603

**Message:** Cannot complete the operation. Access to the server is denied due to a lack of system permissions.

**Explanation:** The user does not have the permissions that are required to complete an operation.

**Recommended Action:** Check to see if the user has the required permissions to access the application server and to complete a backup or restore operation. Ensure that you have added the backup host to the relevant access lists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 6604

**Message:** Failed to complete the operation. The number of open objects on the server has reached its limit.

**Explanation:** There are multiple concurrent jobs running on the application server.

**Recommended Action:** Increase the limit of open objects. To increase the limit of open objects, see the appropriate plug-in support guide. Alternatively, you can check the open file settings on the backup host. For example, `ulimit -n` on UNIX systems.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6605

**Message:** Unable to process the request because the server resources are busy.

**Explanation:** The server resources are either busy or unavailable and this causes the job to fail.

**Recommended Action:** Retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6606

**Message:** Failed to complete the operation. The object already exists.

**Explanation:** The file system folder or the virtual machine already exists.

**Recommended Action:** Do the following, as appropriate:

- If one or more virtual machines exist with the same name, you can either rename or delete one of the virtual machines.
- Check the NetBackup logs (`bpbkar logs` or `nbappdiscv logs`) for more information.
- In addition, you may want to remove the relevant state file.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6607

**Message:** The version of NetBackup does not match the version of the BigData framework libraries.

**Explanation:** There is a version mismatch between NetBackup and the BigData framework libraries.

**Recommended Action:** Ensure that NetBackup and the BigData framework libraries are correctly installed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6608

**Message:** The version of NetBackup does not match the version of the plug-in libraries.

**Explanation:** There is a version mismatch between NetBackup and the plug-in libraries for BigData applications.

**Recommended Action:** Ensure that NetBackup and the relevant plug-in libraries are correctly installed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6609

**Message:** The NetBackup plug-in cannot complete the operation because the object is invalid.

**Explanation:** This error can occur because of the following reasons:

- The application type is either not specified or its value is empty.
- An appropriate plug-in may not be available to complete the operation.

**Recommended Action:** Do the following, as appropriate:

- Check and verify that you have entered the correct entries for the application server or the backup hosts.
- Ensure that you have installed the correct plug-in to successfully complete the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6610

**Message:** An internal error occurred in the NetBackup processes.

**Explanation:** There is an internal error in the NetBackup processes.

**Recommended Action:** Check the NetBackup debug logs for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6612

**Message:** Unable to process the request because the server resources are either busy or unavailable. Retry the operation.

**Explanation:** The application server or the backup host is either busy or unavailable.

**Recommended Action:** Retry the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6614

**Message:** Failed to complete the operation.

**Explanation:** The application server or the backup host shuts down abruptly or crashes while a job is in progress.

**Recommended Action:** Retry the operation after the system is up and running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6616

**Message:** The operation type is currently not supported.

**Explanation:** This error can occur because of the following reasons:

- The selected schedule type is not supported.
- The application server does not support the operation. For example, the snapshot operation may not be supported for certain directories.

**Recommended Action:** Ensure the plug-in supports the type of backups or operations that you are trying to complete.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6617

**Message:** A system call failed.

**Explanation:** An internal error occurred in the application server or the operating system.

**Recommended Action:** Check the system logs or the operating system logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6618

**Message:** NetBackup cannot find the file to complete the operation.

**Explanation:** A file that needs to be backed up is not found or the access permission to the file has changed.

**Recommended Action:** Verify the location of the file. Check if the file was deleted during the backup job. Ensure that the file has the required access permissions.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6619

**Message:** An error occurred because of a network connectivity issue.

**Explanation:** A network problem caused a socket read failure.

**Recommended Action:** To resolve the network connectivity issues, check the system logs and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6620

**Message:** The server has exceeded its connection limit.

**Explanation:** The server has reached the maximum limit of open connections.

**Recommended Action:** Increase the limit of open objects. To increase the limit of open objects, see the appropriate plug-in support guide. Alternatively, you can check the open file settings on the backup host. For example, `ulimit -n` on UNIX systems.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6621

**Message:** An error occurred because the network protocol is not supported.

**Explanation:** The protocol used to communicate with the application server may not be supported.

**Recommended Action:** Verify and resolve any network connectivity issues. To resolve the network connectivity issues, check the system logs and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6622

**Message:** An internal error occurred in the NetBackup process.

**Explanation:** An internal error occurred in the NetBackup process.

**Recommended Action:** Check the NetBackup logs for more details.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6623

**Message:** Failed to connect to the application server or the backup host. The server is either shut down or not reachable.

**Explanation:** This error can occur because of the following reasons:

- The application server is either shut down or it is not reachable.
- The application server was unable to establish a connection with the backup host.

**Recommended Action:** Verify and resolve any network connectivity issues. Ensure that the application server and the backup host are up and running.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6625

**Message:** The backup host is either unauthorized to complete the operation or it is unable to establish a connection with the application server.

**Explanation:** This error can occur because of the following reasons:

- The backup host is not authorized to complete an operation.

- The backup host cannot establish a connection with the application server.
- The backup host is not added to the relevant access lists.

**Recommended Action:** Ensure the following:

- The backup host has the required permissions.
- The firewall issue between the backup host and the application server is resolved.
- The backup host is added to the relevant access lists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6626

**Message:** The server name is invalid.

**Explanation:** The name of the application server is incorrect or invalid.

**Recommended Action:** Ensure that you have provided the correct name for the application server.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6628

**Message:** Unable to establish a network connection due to an error with the Domain Name Service (DNS).

**Explanation:** There is an error within the DNS.

**Recommended Action:** Verify and resolve any network connectivity issues or DNS issues. To resolve the network connectivity issues, check the system logs and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6629

**Message:** Unable to complete the operation. Failed to authorize the user or the server.

**Explanation:** The user or the server is unauthorized to complete an operation.

**Recommended Action:** Ensure that the user has the required permissions and that the server (application server or a backup host) is added to the relevant access lists.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6630

**Message:** Unable to process the request because the server resources are either busy or unavailable. Retry the operation.

**Explanation:** This error can occur because concurrent restore jobs are in progress for the same file or object.

**Recommended Action:** Ensure that a single job is resorting a particular file or an object.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6631

**Message:** There is insufficient storage available to the system.

**Explanation:** The application server or the backup host has insufficient storage available to complete an operation.

**Recommended Action:** Ensure that sufficient storage is available to the system.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6633

**Message:** Unable to complete the operation. Access to the object is denied due to a lack of system permissions.

**Explanation:** You do not have the required permissions to complete an operation.

**Recommended Action:** Ensure that you have read and write access to the file or the object.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6634

**Message:** Unable to find the file or the object.

**Explanation:** A file or an object is either invalid or it does not exist.

**Recommended Action:** Check if the file or the object is available at the specified location. Provide valid entries to complete the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6635

**Message:** The version of the server does not support the requested operation.

**Explanation:** The version of the application server does not currently support the operation that you have requested.

**Recommended Action:** Ensure that the version of the server supports the operation that you have requested.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6640

**Message:** The version of the NetBackup process does not match with the version of the BigData framework libraries.

**Explanation:** There is a version mismatch between NetBackup and its framework libraries.

**Recommended Action:** Ensure that NetBackup and its framework libraries are correctly installed.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6641

**Message:** The relevant libraries are either unavailable or inaccessible.

**Explanation:** The plug-in libraries are either unavailable at the specified location or they do not have the required access permissions.

**Recommended Action:** Ensure that NetBackup and its framework libraries are correctly installed and granted relevant access permissions.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 6642

**Message:** The relevant libraries are either unavailable or the plug-in does not support the requested operation.

**Explanation:** This error occurs because of the following reasons:

- NetBackup is unable to find a specific symbol from a plug-in.
- The plug-in version does not support the operating system or the requested operation.

**Recommended Action:** To resolve this issue, check the NetBackup logs for missing symbols.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6643

**Message:** An internal error occurred in the NetBackup processes.

**Explanation:** The plug-in stopped responding during a backup or a restore job.

**Recommended Action:** Check the NetBackup logs for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6644

**Message:** An internal error occurred in the NetBackup processes.

**Explanation:** This error is an internal error in the NetBackup processes.

**Recommended Action:** Check the system logs or the operating system logs for more information.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6646

**Message:** Unable to communicate with the server.

**Explanation:** You have provided incorrect credentials or invalid inputs for the application server or the backup host.

**Recommended Action:** Ensure that you have entered valid credentials and provided the correct entries (such as the host name and port number) for the application server or the backup host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6647

**Message:** Unable to create or access a directory or a path.

**Explanation:** NetBackup is unable to mount or access a directory or a path.

**Recommended Action:** Ensure that the application server lets the backup host access its files or directories to complete the operations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6649

**Message:** The relevant libraries are either unavailable or inaccessible.

**Explanation:** The plug-in libraries are either unavailable at the specified location or they do not have the required permissions.

**Recommended Action:** Ensure that NetBackup and its framework libraries are correctly installed and have relevant access permissions.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6650

**Message:** The relevant libraries are either unavailable or the plug-in does not support the requested operation.

**Explanation:** This error occurs because of the following reasons:

- NetBackup is unable to find a specific symbol from a plug-in.
- The plug-in version does not support the operating system or the requested operation.

**Recommended Action:** To resolve the issue, check the NetBackup logs for a missing symbol.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6652

**Message:** Failed to complete the operation. The version of the plug-in might not support the requested operation.

**Explanation:** The plug-in libraries do not support the operation that you have requested.

**Recommended Action:** Ensure that the plug-in version supports the operation that you have requested.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6653

**Message:** The selected schedule type is currently not supported.

**Explanation:** Currently, the plug-in does not support the selected schedule type.

**Recommended Action:** When you create a BigData policy, ensure that the plug-in supports the selected schedule type.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6654

**Message:** Unable to retrieve the credentials for the server.

**Explanation:** You have provided invalid credentials to access the application server or the backup host.

**Recommended Action:** Ensure that you have entered valid credentials and provided correct entries for the application server or the backup host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 6655

**Message:** The virtual machine does not exist.

**Explanation:** You have incorrectly provided the display name of the virtual machine.

**Recommended Action:** Enter a valid name for the virtual machine. The virtual machine display name is case sensitive and it does not allow spaces and certain special characters.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7600

**Message:** An unknown internal error occurred.

**Explanation:** The `vnetd` proxy process encountered an internal error.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7601

**Message:** Failed to register service with PBX.

**Explanation:** The `vnetd` HTTP tunnel process failed to register with the Veritas Private Branch Exchange service and is unable to accept incoming connections.

**Recommended Action:** Do the following:

- Verify that the `pbx_exchange` service is running. If not, start the service.
- If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7603

**Message:** Failed to initialize PBX.

**Explanation:** The `vnetd` HTTP tunnel process failed to initialize the Veritas Private Branch Exchange client library and is unable to accept incoming connections.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7604

**Message:** Failed to register PBX acceptor with the reactor.

**Explanation:** The `vnetd` HTTP tunnel process encountered an internal error and is unable to accept incoming connections.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7607

**Message:** Failed to set socket to non-blocking mode.

**Explanation:** The `vnetd` proxy cannot set non-blocking mode on a socket.

**Recommended Action:** If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7609

**Message:** Failed to perform a reactor event handler operation.

**Explanation:** The `vnetd` proxy encountered an internal error and was not able to register for an event notification.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7610

**Message:** Failed to parse the specified object.

**Explanation:** The `vnetd` proxy was not able to parse an object containing details of the request.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7611

**Message:** A connection protocol error occurred.

**Explanation:** The `vnetd` proxy encountered a communication protocol error between endpoints.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7612

**Message:** An unexpected protocol event occurred.

**Explanation:** A protocol error between `vnetd` proxies occurred.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7613

**Message:** A lookup failed for host.

**Explanation:** The `vnetd` proxy failed to complete connection binding for either the source host or the target host in this connection.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7614

**Message:** No valid source-target bindings exist for host.

**Explanation:** The `vnetd` proxy encountered invalid bindings between source and target hosts in this connection.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7617

**Message:** A JSON conversion error occurred.

**Explanation:** The `vnetd` proxy was not able to convert a JSON object to a string.

If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7618

**Message:** Failed to find JSON key.

**Explanation:** The `vnetd` proxy failed to acquire a JSON key.

**Recommended Action:** If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7619

**Message:** The specified state machine is still active.

**Explanation:** The `vnetd` proxy state machine is busy. Requests await processing.

**Recommended Action:** If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7622

**Message:** Input I/O is required.

**Explanation:** The `vnetd` proxy requires socket input to a peer process to satisfy the I/O operation in progress.

**Recommended Action:** Under normal circumstances this message may appear in the logs of the `vnetd` proxy. No user action is required. If a problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7623

**Message:** Output I/O is required.

**Explanation:** The `vnetd` proxy requires socket output to a peer process to satisfy the I/O operation in progress.

**Recommended Action:** Under normal circumstances this message may appear in the logs of the `vnetd` proxy. No user action is required. If a problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7624

**Message:** A SSL socket accept failed.

**Explanation:** The `vnetd` proxy was not able to complete the SSL handshake with the `vnetd` proxy on a remote host.

**Recommended Action:** Examine the details of the error message to determine why the SSL handshake failed. Possible causes of this error may be as follows:

- A missing, expired, or revoked host certificate on the local or the remote host. Verify that the hosts have a valid host ID-based certificate.
- Excessive clock skew on either the local or the remote host. See the information about clock skew in the [NetBackup Security and Encryption Guide](#).
- If you use the NetBackup `SECURE_PROXY_CIPHER_LIST` configuration option on either the local or the remote host, the cipher string entries may be invalid. Verify that the cipher strings are compatible between the hosts.

If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7625

**Message:** A SSL socket connect failed.

**Explanation:** The `vnetd` proxy was not able to complete the SSL handshake with the `vnetd` proxy on a remote host.

**Recommended Action:** Examine the details of the error message to determine why the SSL handshake failed. Possible causes of this error may be as follows:

- A missing, expired, or revoked host certificate on the local or the remote host. Verify that the hosts have a valid host ID-based certificate.
- Excessive clock skew on either the local or the remote host. See the information about clock skew in the [NetBackup Security and Encryption Guide](#).
- If you use the NetBackup `SECURE_PROXY_CIPHER_LIST` configuration option on either the local or the remote host, the cipher string entries may be invalid. Verify that the cipher strings are compatible between the hosts.

If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7627

**Message:** SSL initialization failed.



**Explanation:** The `vnetd` proxy was not able to complete initialization of the SSL environment.

**Recommended Action:** Examine the details of the error message to determine why the SSL handshake failed. Possible causes of this error may be as follows:

- A missing, expired, or revoked host certificate. Verify that the host has a valid host ID-based certificate.
- Excessive clock skew on the host. See the information about clock skew in the [NetBackup Security and Encryption Guide](#).
- If you use the NetBackup `SECURE_PROXY_CIPHER_LIST` configuration option, the cipher string entries may be invalid. Verify that the cipher strings are permitted OpenSSL strings.

If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7628

**Message:** VxSS initialization failed.

**Explanation:** The `vnetd` proxy was not able to complete initialization of the VxSS environment.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7631

**Message:** Certificate path lookup failed.

**Explanation:** The `vnetd` proxy process did not find the path of the host ID certificate.

**Recommended Action:** Verify that the host has a valid host ID-based security certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7632

**Message:** A protocol sanity verification failed.

**Explanation:** The `vnetd` proxy protocol verification failed because it did not receive the expected protocol on a socket.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7633

**Message:** The state machine was terminated before completion.

**Explanation:** The `vnetd` proxy terminated an internal state before it completed.

**Recommended Action:** Under normal circumstances this message may be seen in the logs of the `vnetd` proxy. No user action is required. If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7634

**Message:** Failed to set up a UNIX Domain Socket listener for user.

**Explanation:** A `vnetd` proxy process failed to initialize the listener UNIX Domain Socket.

**Recommended Action:** Examine the status message for additional details. It may be that the process does not have the permissions to create the required files or the disk volume may be full. Examine the state and the contents of `/usr/openv/var/proxy.d` (Linux) or `install_path\Veritas\NetBackup\var\proxy.d` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7635

**Message:** Failed to create a local acceptor.

**Explanation:** A `vnetd` proxy process failed to initialize the acceptor socket.

**Recommended Action:** Examine the status message for additional details. There may be a listen port conflict, or a permission or free space problem with the `proxy.d` directory or its contents. The directory is located in `/usr/openv/var` or `install_path\Veritas\NetBackup\var`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7636

**Message:** Failed to import socket from remote process.

**Explanation:** A `vnetd` proxy process failed to import a socket from another NetBackup process.

**Recommended Action:** This failure is likely a transient problem, perhaps because file descriptors are unavailable temporarily. Therefore, retry the operation. For other root causes, review the `nbpkyhelper` logs or contact NetBackup Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7637

**Message:** Failed to export socket to remote process.

**Explanation:** A `vnetd` proxy process failed to export a socket to another NetBackup process.

**Recommended Action:** This failure is likely a transient problem, perhaps because file descriptors are unavailable temporarily. Therefore, retry the operation. For other root causes, review the `nbpkyhelper` logs or contact NetBackup Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7638

**Message:** Failed to create a socket pair.

**Explanation:** A `vnetd` proxy process failed to create an internal pipe.

**Recommended Action:** This failure is likely a transient problem, perhaps because file descriptors or TCP ports are unavailable temporarily. Therefore, retry the operation. For other root causes, review the `nbpkyhelper` logs or contact NetBackup Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7639

**Message:** Failed to create a peer name mapping.

**Explanation:** The `vnetd` proxy failed to set information in the peer mappings file.

**Recommended Action:** Examine the status message for additional details. It may be that the process does not have the permissions to create the required files or the disk volume may be full. Examine the state and the contents of `/usr/opensv/var/proxy.d` (Linux) or `install_path\Veritas\NetBackup\var\proxy.d` (Windows).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7640

**Message:** The peer closed the connection.

**Explanation:** The peer closed the `vnetd` proxy connection.

**Recommended Action:** Under normal circumstances this message may be seen in the `vnetd` proxy logs. No user action is required. If a problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7641

**Message:** Failed to find a common CA Root for secure handshake.

**Explanation:** The `vnetd` proxy cannot initiate an SSL handshake with the `vnetd` proxy on a remote host because a common certificate authority root cannot be determined.

**Recommended Action:** Examine the error message for the details of which CA Roots each `vnetd` proxy advertised. The following are possible causes of this error:

- **Recommended Action:** Missing, expired, or revoked host certificate on the local or the remote host. Verify that the local and the remote hosts have a valid host ID certificate.
- **Recommended Action:** The hosts are not members of the same NetBackup domain. Ensure that both hosts have host ID certificates issued by the master server intended for the operation.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7642

**Message:** Failed to verify Java GUI session token.

**Explanation:** The `vnetd` proxy cannot validate the session token received from the **NetBackup Administration Console**.

**Recommended Action:** Do the following:

1. Verify the authorization of the user who launched the **NetBackup Administration Console**.  
 See “About authorizing NetBackup users” in the [NetBackup Administrator's Guide, Volume I](#).
2. Close the **NetBackup Administration Console**.
3. Launch a new instance of the **NetBackup Administration Console** and open the **Activity Monitor**.

If the problem persists, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7643

**Message:** Connection cannot be established because the host validation cannot be performed.

**Explanation:** An internal error occurred during the host validation.

**Recommended Action:** If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7645

**Message:** Could not get name from certificate information.

**Explanation:** The `vnetd` proxy cannot extract required information from the remote host ID certificate.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7647

**Message:** Proxy peer does not conform to proxy protocol.

**Explanation:** The `vnetd` proxy cannot validate that its peer is a `vnetd` proxy.

**Recommended Action:** Contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7648

**Message:** Connection cannot be established because the host validation failed.

**Explanation:** The host validation was not successful.

**Recommended Action:** Ensure that the NetBackup master server name and the host name are configured correctly.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7649

**Message:** Data retrieved from the cache is not in a valid format.

**Explanation:** The host validation information obtained from the cache is not in a valid format.

**Recommended Action:** Delete the peer host's cache entry and retry the operation. Use `bpcintcmd -clear_host_cache`. If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7650

**Message:** Data that is retrieved from the server is not in a valid format.

**Explanation:** The host validation information obtained from the master server is not in a valid format.

**Recommended Action:** If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7651

**Message:** Could not process audit reason.

**Explanation:** The `X-NetBackup-Audit-Reason` HTTP header cannot be decoded, possibly because the header was not properly encoded. Non-ASCII characters must be encoded using UTF-8 strings.

**Recommended Action:** Encode the `X-NetBackup-Audit-Reason` HTTP header using the appropriate UTF-8 strings to represent the non-ASCII characters, then resubmit the HTTP web service request.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7652

**Message:** Secure communication proxy is not available for use.

**Explanation:** A `vnetd` secure communication proxy process is not running or available to secure a connection between hosts.

**Recommended Action:** Determine if the `vnetd` process and its proxies are running. On Windows, you can use the **Task Manager Processes** tab (you must show the **Command Line** column). On UNIX and Linux, you can use the NetBackup `bps` command, as follows:

```
$ bpps
...output shortened...
root 13577 1 0 Aug27 ? 00:00:04 /usr/opensv/netbackup/bin/vnetd -standalone
root 13606 1 0 Aug27 ? 00:01:55 /usr/opensv/netbackup/bin/vnetd -proxy inbound_proxy
      -number 0
root 13608 1 0 Aug27 ? 00:00:06 /usr/opensv/netbackup/bin/vnetd -proxy outbound_proxy
      -number 0
```

Depending on which `vnetd` process or proxy is running, try the following:

- If the `vnetd` process (`-standalone`) is not running, start it.
- If the `vnetd` process is running, examine the `vnetd` debug log to confirm that it tries to start the proxy processes.
- If the `vnetd` process does try to start the proxy processes, examine the `nbpxyhelper` debug log to determine why the proxy process does not listen for connections.

If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7653

**Message:** The Peer Certificate is revoked

---

**Note:** This error may also be thrown while logging on to the **NetBackup Administration Console** with a different error message and you will not be able to log in.

---

**Explanation:** The host certificate is present in the CRL and is revoked.

**Recommended Action:** Do the following, as appropriate:

- If the certificate was revoked in error, reissue a certificate for the host.
- If the certificate was revoked as intended, an attempted security breach may have occurred.
- Contact your security administrator.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7654

**Message:** The Certificate Revocation List is invalid

---

**Note:** This error may also be thrown while logging on to the **NetBackup Administration Console** with a different error message and you will not be able to log in.

---

**Explanation:** The revocation status of the host certificate cannot be verified using the Certificate Revocation List (CRL) because the CRL format is not valid.

**Recommended Action:** On the host that has the invalid CRL, run the following command as an administrator to get a fresh CRL:

UNIX:

```
/usr/opensv/netbackup/bin/nbcertcmd -getCRL
```

Windows:

```
install_path\Veritas\Netbackup\bin\nbcertcmd -getCRL
```



Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7655

**Message:** Certificate Revocation List is signed incorrectly

---

**Note:** This error may also be thrown while logging on to the **NetBackup Administration Console** with a different error message and you will not be able to log in.

---

**Explanation:** The signature of the Certificate Revocation List (CRL) does not match the public key of the CA on the master server. The revocation status of the host certificate cannot be verified using the CRL.

**Recommended Action:** The CRL may have been replaced. On the host that has the incorrectly signed CRL, run the following command as an administrator to get a fresh CRL:

UNIX:

```
/usr/opensv/netbackup/bin/nbcertcmd -getCRL
```

Windows:

```
install_path\Veritas\Netbackup\bin\nbcertcmd -getCRL
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7656

**Message:** Certificate Revocation List is out of date

---

**Note:** This error may also be thrown while logging on to the **NetBackup Administration Console** with a different error message and you will not be able to log in.

---

**Explanation:** The revocation status of the host certificate cannot be verified using the Certificate Revocation List (CRL) because the CRL expired. The CRL is older than 7 days.

**Recommended Action:** On the host that has the invalid CRL, run the following command as an administrator to get a fresh CRL:

UNIX:

```
/usr/opensv/netbackup/bin/nbcertcmd -getCRL
```

Windows:

```
install_path\Veritas\Netbackup\bin\nbcertcmd -getCRL
```

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7657

**Message:** Cannot identify service type of acceptor

**Explanation:** The `vnetd` proxy was unable to determine the service type of the acceptor socket.

**Recommended Action:** If the problem persists, contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7658

**Message:** Connection cannot be established because the host validation cannot be performed on the target host.

**Explanation:** An internal error occurred on the remote host while setting up the connection.

**Recommended Action:** If the problem continues, contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7659

**Message:** Connection cannot be established because the host validation failed on the target host.

**Explanation:** The host validation was not successful on the remote host while setting up the connection.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the NetBackup master server name and other host names are correctly configured on the remote host.

- Ensure that the pending mapping requests for this host are approved, or, in the **NetBackup Administration Console**, select the **Security Management > Global Security Settings > Secure Communication > Automatically map NetBackup host ID to host names** option.
- If you have recently installed or upgraded NetBackup, ensure that the security certificates are correctly deployed on all hosts.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 7660

**Message:** The peer proxy cannot find usable certificates for the certificate protocol

**Explanation:** The `vnetd` proxy on the peer host failed to find a usable certificate to complete the certificate protocol.

**Recommended Action:** Verify that certificates have been successfully deployed on the proxy peer host. If the problem occurs after certificates have been deployed successfully, save all the error log information and contact Veritas Technical Support for assistance.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8000

**Message:** User does not have permission(s) to perform the requested operation.

**Explanation:** The user does not have permission(s) to perform the requested operation.

**Recommended Action:** To perform the requested operation, you must be a root user, administrator, or have the appropriate privileges through Enhanced Auditing (EA). Contact the system administrator.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8500

**Message:** Connection with the web service was not established

**Explanation:** The connection with the web service was not established.

**Recommended Action:** Check that the NetBackup Web Management Console is up and running. If it is not running, start it with the `nbwmc -start` command.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8504

**Message:** The web service certificate is issued by an unknown Certificate Authority.

**Explanation:** The certificate presented by the web service is issued by a CA that is not trusted by this host.

**Recommended Action:** Fetch the CA certificate for the required server and rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8505

**Message:** Ensure that the host clock and the master server clock are synchronized.

**Explanation:** A certificate that is not yet valid was found while validating a connection to the web service.

**Recommended Action:** Check if the host's clock is in sync with the specified server. Correct the time on the host, if necessary, and rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8506

**Message:** The certificate has expired.

**Explanation:** An expired certificate was found while validating a connection to the web service.

**Recommended Action:** Check if the host's clock is in sync with the specified server. Correct the time on the host, if necessary, and rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8507

**Message:** The certificate could not be verified.

**Explanation:** The host was not able to verify the certificate.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8508

**Message:** List of trusted Certificate Authorities could not be fetched.

**Explanation:** Trust is not established with any Certificate Authority yet.

**Recommended Action:** Use the `nbcertcmd -listCACertDetails` command to verify that the CA certificate is added to the trust store. Run the `nbcertcmd -getCACertificate -server master_server_name` command to add the required certificate to the trust store.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8509

**Message:** The specified server name was not found in the web service certificate.

**Explanation:** The specified server name does not match any of the host names in the certificate presented by the web service.

**Recommended Action:** Rerun the operation using one of the names listed in the server's certificate.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8510

**Message:** Web server certificate verification failed.

**Explanation:** The host was not able to verify the certificate presented by the web service.

**Recommended Action:** Rerun the operation. If the problem continues, save all of the error log information and contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8617

**Message:** The connection continues because insecure communication with hosts is allowed.

**Explanation:** The peer host is NetBackup 8.0 or earlier and the security setting is configured to allow insecure communication. This setting allows communication with hosts running NetBackup 8.0 or earlier, even though it is insecure.

**Recommended Action:** Upgrade the host to a NetBackup version that is later than 8.0, so it can communicate securely.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8618

**Message:** The connection is dropped because the host ID-to-host name mapping is not approved.

**Explanation:** The host name that is used to connect to another host has not been mapped to the respective host ID and, therefore, the connection is not established.

**Recommended Action:** The NetBackup administrator must approve all relevant host ID-to-host name mappings for the given host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8619

**Message:** The connection continues as the host ID-to-host name mapping is automatically approved.

**Explanation:** The security setting is configured to automatically approve the host ID-to-host name mapping and the connection between the hosts is established.

**Recommended Action:** No action is required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8620

**Message:** The connection is dropped because insecure communication with hosts is not allowed.

**Explanation:** The peer host is NetBackup 8.0 or earlier and the security setting is configured to turn off communication with these hosts and, therefore, the connection is not established.

**Recommended Action:** Upgrade the host to a NetBackup version that is later than 8.0, so it can communicate securely.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8621

**Message:** The connection is dropped because the host appears to be NetBackup 8.0 or earlier.

**Explanation:** The earlier communication status shows that the peer host could communicate securely, but it seems to have been downgraded to NetBackup 8.0 or earlier, and, therefore, the connection is not established.

**Recommended Action:** Verify that the peer host was upgraded and then downgraded to a back-level release. If this is the case, then the NetBackup administrator can mark the given host as insecure.

If this is not the case, then another host is trying to spoof the peer host. You can use the network tools to find out which host it is and take corrective action.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8622

**Message:** The connection is dropped because a conflict in the host ID-to-host name mapping is detected.

**Explanation:** The host ID of the peer host does not match the host ID that is known to the master server and, therefore, the connection is not established. This error can occur in one of the following scenarios:

- In a cluster setup, the active node is down and an inactive node becomes active. Mapping between the host ID of the new active node and the virtual name is not present.
- Two or more hosts in a given NetBackup domain have the same host name.
- An unknown host tries to spoof as the peer host.

**Recommended Action:** If there are multiple host IDs in your environment that are associated with the same host name, the NetBackup administrator should verify and approve the mapping.

If an unknown host tries to spoof the peer host, you can use the available network tools to find out which host it is and take corrective action.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8623

**Message:** Failed to determine the connection type of the host.

**Explanation:** Internal error.

**Recommended Action:** Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8625

**Message:** Server is unavailable to process the request. Please try later.

**Explanation:** This NetBackup status code is accompanied by HTTP status code 503. It indicates one of the following explanations:

- The NetBackup web server is running at full capacity and is unable to process the request. The request fails with a response time of a few milliseconds.
- For a given request, the NetBackup web server has timed out before the response could be fetched from a NetBackup domain service. The NetBackup web services communicate with the domain services such as `nbsl`, `nbaudit`, and `nbemm`. This status code is displayed when there are connection issues with these services. This scenario can be identified by high response times (of approximately 10 minutes) along with this status code.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the NetBackup services are up and running correctly.
- If the relevant NetBackup services are up and you still receive this error code, then the web server is under a heavy load. Retry the operation in a few seconds.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.



## NetBackup status code: 8700

**Message:** The host database web service is unavailable due to an internal error.

**Explanation:** The web service may have encountered an unknown issue on the server-side system. This issue may require further investigation from Veritas Technical Support.

**Recommended Action:** Examine the NetBackup error logs for additional error messages. Additionally, you can refer to the debug logs for this web service (on the master server) to determine the cause of the error.

Alternatively, contact Veritas Technical Support and send the appropriate logs. A complete list of required logs and configuration information is available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8701

**Message:** The host does not exist.

**Explanation:** This error occurs when the host that you want to fetch does not exist. This may happen due to one of the following reasons:

- The host name that you are trying to fetch does not exist.
- The host ID that you are trying to fetch does not exist.

**Recommended Action:** The host that you are trying to access may not be a known NetBackup host. Starting with NetBackup 8.0, a host is added automatically when it communicates with a NetBackup 8.0 master server.

Alternatively, contact Veritas Technical Support and send the appropriate logs. A complete list of required logs and configuration information is available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8702

**Message:** The host cannot be created because the host name already exists in the host database.

**Explanation:** This error occurs due to one of the following reasons:

- The host name that you are trying to create already exists in the host database.
- The host ID that you are trying to create already exists in the host database.

**Recommended Action:** To resolve issues that are related to different hosts having the same name or alias, verify the network host name mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8703

**Message:** The host cannot be created because the host ID-to-host name mapping already exists in the host database.

**Explanation:** The host name conflicts with an alias name that already exists in the database in a case insensitive comparison. You can find the host ID of the existing host or alias in the Location field of the response header.

**Recommended Action:** To resolve issues that are related to different hosts having the same name or alias, verify the network host name mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8704

**Message:** A conflict occurred while updating the host database. Kindly retry the operation.

**Explanation:** This error occurs when you try to create or modify the host database at the same time.

**Recommended Action:** Retry the operation. If the problem continues, contact Veritas Technical Support and send the appropriate logs. A complete list of required logs and configuration information is available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8706

**Message:** The required field is missing from the input request.

**Explanation:** Entering a value for the given field is mandatory to complete the operation.

**Recommended Action:** Enter a valid value for the mandatory fields and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8707

**Message:** The web service cannot update the host ID.

**Explanation:** This error occurs when you try to modify a host ID. You cannot update the host ID because it is the unique identifier of a NetBackup host.

**Recommended Action:** Remove the host ID from the input request to complete the remaining operations.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8708

**Message:** Constraint violations are detected for the given attributes in the input request

**Explanation:** The error message points to an erroneous input parameter and displays the constraint that failed for the parameter. For example, the input value for the input parameter is a string; however, you entered an integer.

**Recommended Action:** Enter a valid input for the input parameter and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8709

**Message:** The destination file or directory already exists.

**Explanation:** Telemetry data for the host already exists on the server.

**Recommended Action:** No action required.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8710

**Message:** The file cannot be uploaded because of insufficient disk space on the host.

**Explanation:** The server may not have enough disk space to store the telemetry file.

**Recommended Action:** To resolve the issue, create space on the master server for *var/global* paths.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8711

**Message:** The folder where the telemetry data needs to be uploaded does not exist.

**Explanation:** This error indicates that the destination folder, where the telemetry data is uploaded, is missing.

**Recommended Action:** Contact Veritas Technical Support and send the appropriate logs. A complete list of required logs and configuration information is available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8712

**Message:** Failed to upload the file.

**Explanation:** An error occurred while uploading the telemetry file.

**Recommended Action:** Contact Veritas Technical Support and send the appropriate logs. A complete list of required logs and configuration information is available.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8713

**Message:** Failed to upload the file. The input file cannot be empty.

**Explanation:** The input file is empty; therefore, the telemetry data cannot be uploaded.

**Recommended Action:** Verify that the input file for telemetry is correct.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8714

**Message:** The mapping cannot be marked as unshared because it is already shared.

**Explanation:** A host ID-to-host name mapping that is already shared cannot be marked as unshared.

**Recommended Action:** Delete the shared mapping entry.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8715

**Message:** A conflict in the mapping is detected. The host name is already mapped with a different host.

**Explanation:** The mapping cannot be added as there is a conflict. The host name is already mapped with a different host.

**Recommended Action:** Do one of the following to resolve the conflicting mapping:

- Mark the conflicting mapping as shared to be able to approve it.
- Delete the conflicting mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8716

**Message:** The mapping cannot be added because it is empty.

**Explanation:** An empty host ID-to-host name mapping cannot be added.

**Recommended Action:** Provide a valid host ID-to-host name mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8717

**Message:** The operation failed as one of the input parameters is invalid.

**Explanation:** One of the input parameters is invalid.

**Recommended Action:** Provide a valid input parameter. For more information, see the NetBackup logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8718

**Message:** The mapping cannot be deleted as this is the primary host name for the host ID.

**Explanation:** The host ID-to-host name mapping cannot be deleted if it is the primary host name that is mapped with the host ID.

**Recommended Action:** Do not delete the primary host name that is mapped with the host ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8719

**Message:** The conflicting mapping cannot be approved because it is not a shared mapping.

**Explanation:** A conflicting mapping can be approved only if it is shared.

**Recommended Action:** Do one of the following to resolve the conflicting mapping:

- Mark the conflicting mapping as shared to be able to approve it.
- Delete the conflicting mapping.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8720

**Message:** The host ID does not exist.

**Explanation:** The master server does not recognize the specified host ID.

**Recommended Action:** Check the specified host ID by using the `nbcertcmd -listCertDetails` command. If the specified NetBackup host is part of multiple NetBackup domains, ensure that you provide the correct host ID that corresponds to the specified NetBackup domain.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8722

**Message:** The specified name exceeds the maximum allowed length of 1024 characters. Enter a valid name for host ID-to-host name mapping.

**Explanation:** A host ID-to-host name mapping can contain up to 1024 characters.

**Recommended Action:** Ensure that the mapping that you have entered does not exceed 1024 characters.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8723

**Message:** The specified comment exceeds the maximum allowed length.

**Explanation:** A comment can contain up to 2048 bytes.

**Recommended Action:** Ensure that the comment that you provide does not exceed 2048 bytes.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8724

**Message:** The host ID-to-host name mapping cannot be configured as a shared mapping because it is associated with a single host.

**Explanation:** Only host ID-to-host name mappings that are shared across multiple hosts (for example, in cluster or multi-domain scenarios) should be configured as shared mappings.

**Recommended Action:** Ensure that the host ID-to-host name mapping that you want to add is not configured as shared because the mapping is associated with a single host.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8800

**Message:** Communication with EMM failed.

**Explanation:** NetBackup attempted a request that requires communication with `nbemm` and the communication with `nbemm` failed.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the `nbemm` service is running.
- Restart `nbemm` or the NetBackup Web Management Console (`nbwmc`) and retry the request.

- Examine the unified logging files on the NetBackup master server for the `nbeumm` (OID 111) service and the NetBackup web services. Unified logging is written to `/usr/openv/logs` (UNIX) or to `install_path\NetBackup\logs` (Windows). See the [NetBackup Troubleshooting Guide](#) and the [NetBackup Logging Reference Guide](#) for details on troubleshooting the web services and on their logs.
- If the problem persists, contact customer support and provide the appropriate logs.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8900

**Message:** The host name that was provided must be associated with a single host ID.

**Explanation:** This error occurs when the host name that you want to add or delete for mapping is associated with multiple host IDs.

**Recommended Action:** Ensure that the host name that you want to add or delete for mapping is associated with a single host ID.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8901

**Message:** The mapping name that was provided does not exist.

**Explanation:** This error occurs when the mapping name that you want to fetch does not exist.

**Recommended Action:** Provide a valid mapping name and try again.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 8902

**Message:** Mappings for the specified host do not exist.

**Explanation:** The specified host does not exist or the mappings for the host do not exist.

**Recommended Action:** Provide a valid host name and try again.



Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9101

**Message:** Failed to lock the file.

**Explanation:** This error can be due to the following reasons:

- NetBackup cannot create the lock file, perhaps due to a permissions error.
- The file is locked by another process.

**Recommended Action:** Do the following, as appropriate:

- Examine the logs for the operation you tried to perform.
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- On all hosts involved in the communication, examine the unified logs for `nbpxyhelper` (OID 486).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9102

**Message:** Failed to unlock the file.

**Explanation:** NetBackup was not able to unlock the file for editing.

**Recommended Action:** Do the following, as appropriate:

- Examine the logs for the operation you tried to perform.
- Examine legacy logs on the NetBackup server for `nbcertcmd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9103

**Message:** Unexpected response from the web service.

**Explanation:** This error can be due to the following reasons:

- The client failed to parse the HTTP response from the master server.
- The client may have made a web service request to a back-level master server.

**Recommended Action:** Do the following, as appropriate:

- Upgrade the back-level master server.

- On the master server, examine the unified logs on the NetBackup server for `nbwebservice` (all OIDs).
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- On all hosts involved in the communication, examine the unified logs for `nbpxyhelper` (OID 486).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9300

**Message:** Failed to encode the certificate revocation list (CRL).

**Explanation:** NetBackup encountered an OpenSSL issue when it attempted to encode a CRL into PEM or DER.

**Recommended Action:** Do the following, as appropriate:

- On the master server, examine the unified logs on the NetBackup server for `nbwebservice` (OID 466 and 484).
- On all hosts involved in the communication, examine the unified logs for `nbpxyhelper` (OID 486).
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- Ensure that you use the NetBackup SSL libraries.
- Contact Veritas Technical Support.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9301

**Message:** Failed to decode the certificate revocation list (CRL).

**Explanation:** This error can be due to the following reasons:

- The PEM- or DER-encoded CRL is malformed or empty.
- The master server returned an invalid CRL when the host tried to fetch the CRL via an HTTP request.
- NetBackup encountered an OpenSSL issue when it attempted to decode a PEM- or a DER-encoded CRL.

**Recommended Action:** Do the following, as appropriate:

- On the master server, examine the unified logs on the NetBackup server for `nbwebsservice` (OID 466 and 484).
- On all hosts involved in the communication, examine the unified logs for `nbpxyhelper` (OID 486).
- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- Run the following command to get a new CRL for the corresponding domain:  
`./nbcertcmd -getCrl [-server master server name]`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9302

**Message:** Attempted to replace the certificate revocation list (CRL) with an older version.

**Explanation:** NetBackup attempted to write a CRL that is older than the existing CRL.

**Recommended Action:** Do the following, as appropriate:

- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- On all hosts involved in the communication, examine the unified logs for `nbpxyhelper` (OID 486).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9303

**Message:** The web service request to fetch the certificate revocation list (CRL) failed.

**Explanation:** This error can be due to the following reasons:

- The HTTP request to get the CRL did not return a success (200) status code.
- The HTTP request timed out.

**Recommended Action:** Do the following, as appropriate:

- On the host where the error occurred, examine the legacy logs for `nbcertcmd`.
- On the master server, examine the unified logs on the NetBackup server for `nbwebsservice` (OID 466 and 484).
- Ensure the following:

- The master server is online.
- The web service (`nbwmc`) is online.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9304

**Message:** The HTTP request is not complete; it should be checked again later.

**Explanation:** The HTTP request to fetch the CRL or the security level is not complete; it should be checked again later.

**Recommended Action:** Examine the legacy logs for `nbcertcmd` and the unified logs on the NetBackup server for `nbwebsservice` (OID 466 and 484).

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9305

**Message:** An attempt to refresh the certificate revocation list (CRL) and security level was partially successful.

**Explanation:** When `nbcertcmd` tries to refresh CRL, it performs the following steps:

1. Send the HTTP request to fetch the CRL.
2. Deploy the CRL.
3. Send the HTTP request to fetch the security level.
4. Deploy the security level.

This error can be due to the following reasons during this operation:

- The host fetched the CRL, but failed to deploy the CRL or failed to fetch or deploy the security level.
- The host fetched the security level but failed to deploy the security level or failed to fetch or deploy the CRL.

**Recommended Action:** Do the following, as appropriate:

- Examine the legacy logs for `nbcertcmd`.
- Ensure that the HTTP request to fetch the CRL and the security level was successful. On the NetBackup server, examine the unified logs for `nbwebsservice` (OID 466 and 484) for HTTP request failures.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9306

**Message:** The HTTP request for fetching the security level failed.

**Explanation:** This error can be due to the following reasons:

- The HTTP request to get the security level did not return a success (200) status code.
- The HTTP request timed out.
- The HTTP request failed due to an unknown reason.

---

**Note:** This error code is returned only if the HTTP request fails for all of the servers.

---

**Recommended Action:** Do the following, as appropriate:

- Examine the legacy logs for `nbcertcmd` and the unified logs on the NetBackup server for `nbweb service` (OID 466 and 484).
- Ensure the following:
  - The master server is online.
  - The web service (`nbwmc`) is online.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9307

**Message:** The HTTP request to fetch the CRL failed. The reason for the failure is unknown.

**Explanation:** This error code is returned when the reason for the CRL HTTP request failure is unknown.

**Recommended Action:** Examine the legacy logs on the NetBackup host for `nbcertcmd`.

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9308

**Message:** Failed to read the certificate revocation list (CRL).

**Explanation:** The CRL is not present or there was an issue reading it.

**Recommended Action:** Do the following, as appropriate:

- On all hosts involved in the communication, examine the unified logs for `nbpkyhelper` (OID 486).
- Examine the legacy logs for `nbcertcmd`.
- For a Windows server, verify that the following directories exist:  
`install_path\NetBackup\var\vxss\crl`  
For a clustered master server:  
`install_path\NetBackup\var\global\vxss\crl`
- For a UNIX server, verify that the following directories exist:  
`/usr/opensv/var/vxss/crl`  
For a clustered master server:  
`/usr/opensv/var/global/vxss/crl`
- For a Windows server, verify in the `certmapinfo.json` files that the `crlPath` values point to a valid path for the CRL:  
`install_path\NetBackup\var\vxss\certmapinfo.json`  
For a clustered master server:  
`install_path\NetBackup\var\global\vxss\certmapinfo.json`
- For a UNIX server, verify in the `certmapinfo.json` files that the `crlPath` values point to a valid path for the CRL:  
`/usr/opensv/var/vxss/certmapinfo.json`  
For a clustered master server:  
`/usr/opensv/var/global/vxss/certmapinfo.json`
- Run the following command for the master server:  
`./nbcertcmd -getCRL -server master_server_name`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup status code: 9309

**Message:** Failed to write the certificate revocation list (CRL).

**Explanation:** There was an issue writing the CRL file.

**Recommended Action:** Do the following, as appropriate:

- Examine the unified logs on the NetBackup server for `nbweb service` (OID 466 and 484) and the legacy logs for `nbcertcmd`.
- For a Windows server, verify that the following directories exist:  
`install_path\NetBackup\var\vxss\crl`  
For a clustered master server:  
`install_path\NetBackup\var\global\vxss\crl`
- For a UNIX server, verify that the following directories exist:  
`/usr/openv/var/vxss/crl`  
For a clustered master server:  
`/usr/openv/var/global/vxss/crl`

Click [here](#) to view technical notes and other information in the Veritas Knowledge Base about this status code.

## NetBackup KMS status codes

The following is a complete list of the NetBackup Key Management Service (KMS) status codes that are listed in numerical order:

---

**Note:** The '%' sign in the error messages is a place holder for the error string that would be displayed when you run that particular command.

---

For more information about each command, see the [NetBackup Commands Reference Guide](#).

### NetBackup KMS status code: 1

**Message:** Failed to initialize the ORB

**Explanation:** Internal error

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

### NetBackup KMS status code: 2

**Message:** Failed to create a new Key Group

**Explanation:** A key group with the same name already exists or the key group name is not supported.

**Recommended Action:** Try to create another key group with a different name.

## NetBackup KMS status code: 3

**Message:** Failed to create a new Key

**Explanation:** The key already exists or the key name is not supported

**Recommended Action:** Provide a valid key group name or try to create another key with a different name.

## NetBackup KMS status code: 4

**Message:** Failed to modify Key Group details

**Explanation:** The modification can fail because of the following reasons:

- The key group does not exist.
- A key group with the name you provided already exists.

**Recommended Action:** Provide a valid key group name or create another key group with a different name.

## NetBackup KMS status code: 5

**Message:** Failed to modify Key details

**Explanation:** The key does not exist. The name you provided already exists.

**Recommended Action:** Provide a valid key name or try to create another key with a different name.

## NetBackup KMS status code: 6

**Message:** Failed to delete the Key Group

**Explanation:** You can only delete empty key groups.

**Recommended Action:** Delete all the keys from that group and then try to delete that key group. If required, you can also force delete a key group even if it is not empty. Use the `-force` option to delete the key group.

## NetBackup KMS status code: 7

**Message:** Failed to fetch Key Group details

**Explanation:** The required key group does not exist in the database.

**Recommended Action:** Provide a valid key group name and try again.



## NetBackup KMS status code: 8

**Message:** Failed to fetch Key(s) details

**Explanation:** The required key or keys do not exist in the database.

**Recommended Action:** Provide a valid key name

## NetBackup KMS status code: 9

**Message:** Failed to fetch Key Store statistics

**Explanation:** The failure can be as:

- The keystore (KMS database) does not exist
- The KMS service is down

**Recommended Action:** Create a KMS database (keystore). Restart the KMS service.

## NetBackup KMS status code: 10

**Message:** Failed to modify Host Master Key

**Explanation:** The passphrase or ID is incorrect.

**Recommended Action:** Provide the correct ID and passphrase.

## NetBackup KMS status code: 11

**Message:** Failed to modify Key Protection Key

**Explanation:** The passphrase or ID is incorrect.

**Recommended Action:** Provide the correct ID and passphrase.

## NetBackup KMS status code: 12

**Message:** Failed to register OBVs with ORB

**Explanation:** Internal error.

**Recommended Action:** Please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 13

**Message:** Request timed out. NBSL service might be down.

**Explanation:** The timeout can be due to the following reasons:

- The user does not have the required permissions
- The NBSL service must be down

**Recommended Action:** Restart the NBSL service.

## NetBackup KMS status code: 14

**Message:** Failed to establish a session with NBSL

**Explanation:** The service fails to establish a session with NBSL. There must be an invalid reference to the NBSL session.

**Recommended Action:** Restart the NBSL service.

## NetBackup KMS status code: 15

**Message:** Failed to get Modifiable Facet Instance. KMS service might be down.

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 16

**Message:** Failed to narrow to Modifiable Facet Instance

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 17

**Message:** Failed to get Queryable Facet Instance. KMS service might be down

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 18

**Message:** Failed to narrow to Queryable Facet Instance

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 19

**Message:** Failed to get Control Facet Instance. KMS service might be down.

**Explanation:** Unable to invoke some KMS API.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 20

**Message:** Failed to narrow to Control Facet Instance

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 21

**Message:** Failed to get Exim Facet Instance. KMS service might be down.

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 22

**Message:** Failed to narrow to Exim Facet Instance

**Explanation:** Internal error.

**Recommended Action:** Restart the KMS service. If the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 23

**Message:** New Key Group creation is successful

**Explanation:** The new key group was created successfully.

**Recommended Action:** No action required.

## NetBackup KMS status code: 24

**Message:** New Key creation is successful

**Explanation:** The new key was created successfully.

**Recommended Action:** No action required.

## NetBackup KMS status code: 25

**Message:** Key Group details are updated successfully

**Explanation:** Key group details were updated successfully.

**Recommended Action:** No action required.

## NetBackup KMS status code: 26

**Message:** Key details are updated successfully

**Explanation:** Key details were updated successfully.

**Recommended Action:** No action required.

## NetBackup KMS status code: 27

**Message:** Key Group deletion is successful

**Explanation:** Key group successfully deleted.

**Recommended Action:** No action required.

## NetBackup KMS status code: 28

**Message:** No Key Groups were found

**Explanation:** There are no key groups with the specified name or those key groups do not exist.

**Recommended Action:** Create the required key groups or try to list them with the correct name.

## NetBackup KMS status code: 29

**Message:** No Keys were found

**Explanation:** There were no keys in the database to be listed.

**Recommended Action:** Create the required keys first.

## NetBackup KMS status code: 30

**Message:** Host Master Key update is successful

**Explanation:** Host Master Key successfully updated.

**Recommended Action:** No action required.

## NetBackup KMS status code: 31

**Message:** Key Protection Key update is successful

**Explanation:** Key Protection Key successfully updated.

**Recommended Action:** No action required.

## NetBackup KMS status code: 32

**Message:** Missing or duplicate option: %s

**Explanation:** You missed an option or the option is duplicated.

**Recommended Action:** Use or add the missing option or remove the duplicate option.

For complete information on all of the NetBackup commands, see the [NetBackup Commands Reference Guide](#).

## NetBackup KMS status code: 33

**Message:** All of the options are mutually exclusive

**Explanation:** The options you used are mutually exclusive.

**Recommended Action:** Use a single option.

## NetBackup KMS status code: 34

**Message:** Options %s %s are mutually exclusive

**Explanation:** The %s and %s options are mutually exclusive.

**Recommended Action:** Use a single option.

## NetBackup KMS status code: 35

**Message:** Invalid option or value: %s

**Explanation:** The option %s is not valid in this context (command).

**Recommended Action:** Please provide valid options for this context (command).

## NetBackup KMS status code: 36

**Message:** Unknown option used

**Explanation:** The option that you used is not valid.

**Recommended Action:** Please check the value of the option (can also be a spelling mistake) or provide a valid value.

## NetBackup KMS status code: 37

**Message:** Invalid value for %s: %s

**Explanation:** The cipher value must not be valid.

**Recommended Action:** Please provide a valid value.

## NetBackup KMS status code: 38

**Message:** Invalid value for %s: %s

**Explanation:** The state value is not valid.

**Recommended Action:** Please provide a valid value.

## NetBackup KMS status code: 39

**Message:** Invalid operation

**Explanation:** You used an invalid command.

**Recommended Action:** Please check the [NetBackup Commands Reference Guide](#).

## NetBackup KMS status code: 40

**Message:** Failed to get Key Group details

**Explanation:** A key group with the given name does not exist in the KMS database.

**Recommended Action:** Check if that key group exists in the KMS database.

## NetBackup KMS status code: 41

**Message:** Failed to get Host Master Key ID

**Explanation:** The host master key contains the encryption key that encrypts and protects the KMS data.

**Recommended Action:** Make sure that a valid keystore file is present.

## NetBackup KMS status code: 42

**Message:** Failed to get Key Protection Key ID

**Explanation:** A Protection Key is used to encrypt the keys. This operation may be called when the keystore is either initialized or not initialized. A valid keystore file must be present for this call to succeed.

**Recommended Action:** Make sure that a valid keystore file is present. If the problem persists please contact NetBackup Support.

## NetBackup KMS status code: 44

**Message:** Failed to get KMS service manager instance

**Explanation:** Unable to connect to the KMS service manager because of the following:

- KMS service manager is busy.
- KMS service manager has restarted.
- KMS service manager has stopped.

**Recommended Action:** Retry after a few minutes. If the KMS service manager has stopped, please restart the service.

## NetBackup KMS status code: 45

**Message:** Failed to quiesce Keystore

**Explanation:** A quiesce sets the keystore in a read-only mode for backup.

**Recommended Action:** Retry after a few minutes; if the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 46

**Message:** Failed to unquiesce Keystore

**Explanation:** A quiesce sets the keystore in a read-only mode for backup; unquiesce operation restores it to normal state.

**Recommended Action:** Retry after a few minutes; if the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 47

**Message:** Failed to get keystore quiesce status

**Explanation:** Keystore quiesce operation failed.

**Recommended Action:** Retry after a few minutes; if the problem persists, please contact NetBackup Support and provide the relevant supporting materials.

## NetBackup KMS status code: 48

**Message:** Key Store quiesce is successful

**Explanation:** No problems were detected with the requested operation.

**Recommended Action:** No action needed.

## NetBackup KMS status code: 49

**Message:** Key Store unquiesce is successful

**Explanation:** No problems were detected with the requested operation.

**Recommended Action:** No action needed.

## NetBackup KMS status code: 50

**Message:** Failed recover Key with known Tag

**Explanation:** The key cannot be recovered with the tag that you provided. A single KMS database cannot have two keys with the same tag. The key possibly (with the key tag you provided) already exists in the database.

**Recommended Action:** Delete the existing key and then try to recover the key or cancel the key recovery operation depending on the requirement.

## NetBackup KMS status code: 51

**Message:** Key recovery is successful

**Explanation:** Successfully recovered the required key.

**Recommended Action:** No action needed.

## NetBackup KMS status code: 52

**Message:** Failed to delete the Key

**Explanation:** Key deletion has failed. A possibility is that you did not provide the correct key (`-keyname`) and key group (`-kgname`) combination.

**Recommended Action:** Verify that you have provided the correct key and key group combination and then try to delete the key.



## NetBackup KMS status code: 53

**Message:** Key deletion is successful

**Explanation:** The key is successfully deleted.

**Recommended Action:** No action needed.

## NetBackup KMS status code: 54

**Message:** Authentication failed check NBAC credentials

**Explanation:** The user might not have the required permissions.

**Recommended Action:** Use an account that has the correct access permission for this NBAC operation. You can also add the user to right NBAC group and then try again.

## NetBackup KMS status code: 55

**Message:** Access denied on this operation check NBAC permissions

**Explanation:** The user might not have the required permission.

**Recommended Action:** Use an account that has the correct access permission for this NBAC operation. You can also add the user to right NBAC group and then try again.

## NetBackup KMS status code: 56

**Message:** Authorization failed check NBAC credentials

**Explanation:** The user might not have the required permissions.

**Recommended Action:**

## NetBackup KMS status code: 57

**Message:** Nothing to modify

**Explanation:** Invalid combination of options in user command.

**Recommended Action:** Verify combination of options in your command.

## NetBackup KMS status code: 58

**Message:** Keystore successfully exported

**Explanation:** Keystore is successfully exported.

**Recommended Action:** No action is needed.

## NetBackup KMS status code: 59

**Message:** Failed to export keystore

**Explanation:** The error is caused by the following reasons:

- Failed to open key list file
- Failed to export keystore file
- Specified file already exists
- Failed to open secure keystore file
- Failed to write to secure keystore file

**Recommended Action:** Check the permissions where the exported file is saved. If the file already exists, export it with a different name.

## NetBackup KMS status code: 60

**Message:** Successfully imported keystore file

**Explanation:** The keystore file is successfully imported.

**Recommended Action:** No action needed.

## NetBackup KMS status code: 61

**Message:** Failed to import keystore file into the KMS Database

**Explanation:** The keystore import fails due to the following reasons:

- The secure keystore file cannot be opened
- There was an error reading the contents of the secure keystore file (incorrect format).
- Keystore file import failed.

During an import, when you import key groups with the `[-preserve_kgname]` option and that group already exists in KMS, the entire operation fails.

NetBackup KMS has a limit of 100 key groups. Each group has a limit of 30 keys. The operation fails if more than 100 key groups are imported.

**Recommended Action:** Take the following actions, depending on the scenario:

- Make sure that a valid keystore file is present.

- You must either delete or rename the existing key groups or exclude the `[-preserve_kgname]` option and rerun the import operation.
- You must delete existing unwanted key groups and rerun the import operation.

## NetBackup KMS status code: 62

**Message:** Failed to read file. Please check the format and try again.

**Explanation:** The read operation failed as the format of the file was incorrect.

**Recommended Action:** Please check the format of the file and try again.

## NetBackup KMS status code: 63

**Message:** You must provide the Salt value to recover the key

**Explanation:** For 7.7 and later versions, a salt is always generated when you create a new key. The same salt value must be provided when you want to recover that key.

**Recommended Action:** For recovery, you must provide the salt value of the deleted key if it was created with NetBackup 7.7 or later versions.

## NetBackup KMS status code: 1287

**Message:** Invalid characters found in name: %s\n -- Valid character set: A-Z a-z 0-9, \_, -, ., :, and space -- Name should start with A-Z or a-z or 0-9

**Explanation:** Some unsupported characters were detected in the given name or the name is not in an acceptable format.

**Recommended Action:** Provide the name in the correct format.

# Media Manager status codes

This chapter includes the following topics:

- [Media Manager status codes](#)

## Media Manager status codes

These status codes appear in the following: exit status and command output for most media and device management commands, media and device management user interfaces, and system or debug logs.

### Media Manager status code 1

**Message:** request completed

**Explanation:** A requested operation was completed. The operation may have been one of several related operations for a particular task.

**Recommended Action:** None

### Media Manager status code 2

**Message:** system error

**Explanation:** A system call failed. This status code is used for a generic system call failure that does not have its own status code.

**Recommended Action:**

- Check for other error messages in the command or the interface output to determine which system call failed.

- Check the system application log for error and warning messages.
- Verify that the system is not running out of virtual memory. If virtual memory is the problem, shut down unused applications or increase the amount of virtual memory.

To increase virtual memory on Windows, do the following in the order presented:

- Display the Control Panel.
- Double-click **System**.
- On the **Performance** tab, set **Virtual Memory** to a higher value.
- Verify that all of the product binaries are properly installed.
- Verify that no unexpected media and device management processes are in operation by running `vmps`. Some processes are expected to continue running. Others that continue to run can indicate a more serious problem, such as a hung system call.

## Media Manager status code 3

**Message:** user ID was not superuser

**Explanation:** A user or process that did not have root privileges (on UNIX and Linux) or administrator privileges (on Windows) started the process.

**Recommended Action:** If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX and Linux) and retry the operation.

## Media Manager status code 4

**Message:** invalid command usage

**Explanation:** A media and device management command was run with improper options, or an incompatibility between components or versions of the product exists.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the usage statement for expected usage and compare with the parameters being sent to start the new process.
- Verify that all media and device management binaries are at a compatible version level.

## Media Manager status code 5

**Message:** daemon resources are busy

**Explanation:** A requested operation cannot be processed because resources were busy.

**Recommended Action:** Check the status of any resources that the requested operation uses. On a robotic inventory request, verify that the inventory operation completes within a reasonable time.

## Media Manager status code 6

**Message:** invalid protocol request

**Explanation:** An invalid request was sent to a robotic process or operator request process.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the target components (for example, `vmd`, `nbemm`, and robotic processes on local or remote hosts). Then, verify that all of the media and device management binaries are at a compatible version level.

## Media Manager status code 7

**Message:** daemon terminated

**Explanation:** The process is inactive or terminates (or has terminated) from the following: an event or signal or as a direct result of a request from an authorized user or process.

**Recommended Action:** If the targeted product component is needed but has terminated, restart the daemons or services on the targeted host.

## Media Manager status code 8

**Message:** invalid media ID

**Explanation:** When a process performed a media-related operation, it encountered an empty or an incorrectly formatted media identifier. Or a media ID that was passed to it cannot be operated on as requested.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the media ID, where requested, is not blank.
- Ensure that the specified media IDs contain valid characters only: alphanumeric characters, the period (.), the plus sign (+), and the underscore (\_). A hyphen (-) is also a valid character when not the first character in the media ID.
- If media are specified to be ejected from a library, ensure the following: they exist in the EMM database and are associated with the correct robot number.
- Ensure that the media ID is from 1 to 6 characters in length.
- Ensure that a valid media and seed were specified.
- If the operation is an inventory request for an ACS robot, use the `robtest` utility to verify the following: the ACS interface returns cleaning media IDs both in the query volume list and in the query cleaning volume list.

## Media Manager status code 9

**Message:** invalid media type

**Explanation:** A process that performed a media-related operation encountered an unknown, missing, or incompatible media type specifier.

**Recommended Action:**

- If you run a robot inventory on a robot of type ACS, TLH, or TLM, ensure that the installed version of NetBackup supports and recognizes the vendor media type that the robot control software returns.
- If using a command-line interface directly, verify that a valid media type has been passed, according to `vmadd (1m)` command-line documentation.
- Ensure that an operation valid only for cleaning media has not been requested on a media ID that does not correspond to the cleaning tape.
- Ensure that the media type in all barcode rules is a valid media type or the ordinal zero (0), to represent the default media type.

## Media Manager status code 10

**Message:** invalid barcode

**Explanation:** When a process performed a media-related operation, it encountered an unknown, missing, or incompatible barcode.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the barcode, where requested, is not blank.
- Ensure that the specified barcodes only contain the following valid characters: alphanumeric characters, the period (.), plus sign (+), and underscore (\_). A hyphen (-) is also a valid character when it is not the first character in the media ID.
- Ensure that the number of characters in the barcode does not exceed the maximum that is allowed for the robot type.
- Ensure that the barcode tag in all of the barcode rules is a subset of a valid, supported barcode format.

## Media Manager status code 11

**Message:** invalid description

**Explanation:** The volume description exceeds 25 ASCII characters in length, or contains unprintable characters.

**Recommended Action:** When you add or change a volume record or barcode rule record, ensure that the description field contains the following: no more than 25 ASCII characters that can be printed.

## Media Manager status code 12

**Message:** invalid robot type

**Explanation:** A requested operation encountered a case where a specified robot type or a volume's robot type is different. It differs from the type of robot that is required to perform the operation in the current configuration.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a robot type that supports the volume's media type.



- Check the EMM database and ensure that the specified robot type agrees with the type for all volumes having the specified robot number.
- If a robot type is required for the requested operation, ensure that a robot type has been specified.

## Media Manager status code 13

**Message:** invalid robot number

**Explanation:** The robot number was not specified or was not within the allowable range.

**Recommended Action:**

- Specify a robot number in the range from 0 to 32767.
- If you run `vmphyinv`, the global device database may not be updated, or the specified robot number may not be configured.

## Media Manager status code 14

**Message:** invalid robot host

**Explanation:** A requested operation encountered a case where the following is true of the robot control host:

- It is not specified.
- It is not valid for the given robot type.
- It is not in an acceptable format.
- It exceeds the allowed length of a robot control host name.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- If possible, attempt the requested operation again with another user interface that supports the type of request.

## Media Manager status code 15

**Message:** invalid volgroup

**Explanation:**

A requested operation encountered a case where the volume group:

- Is not specified
- Is not in an acceptable format
- Exceeds the allowed length of a volume group name

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a volume group where one is required to ensure that it contains the following:
  - 25 ASCII characters or less
  - No white space
  - No unprintable characters

## Media Manager status code 16

**Message:** invalid robot coord1

**Explanation:** A requested operation encountered a missing or out-of-range robot slot number. Or a move by volume group residence was attempted when the volume did not originate from a valid robotic library slot.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a slot number (robot coordinate 1) where required and ensure that the number is within the allowable range for the given robot type.

## Media Manager status code 18

**Message:** cannot allocate requested memory

**Explanation:** The allocation of system memory failed. This error occurs when insufficient system memory is available. The system may have too little physical and virtual memory to handle the current load of processes.

**Recommended Action:** Free up memory by terminating any unneeded processes that consume a lot of memory. Add more swap space or physical memory.

## Media Manager status code 19

**Message:** invalid database host

**Explanation:** A requested operation encountered a missing or an invalid database host. Or a request was sent to a host that is running a version of the product that does not support the requested operation.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a valid EMM database host on which the following is running: a version of `nbeemm` (the NetBackup Enterprise Media Manager) or an operator request daemon or process that supports the requested operation.

## Media Manager status code 20

**Message:** protocol error

**Explanation:** Message communications (handshaking) was not correct.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the logs. Ensure that no whitespaces are embedded in the fields that do not allow embedded whitespace.

## Media Manager status code 21

**Message:** cannot obtain daemon lockfile

**Explanation:** `vmd` (NetBackup Volume Manager daemon on UNIX and Linux; NetBackup Volume Manager service on Windows) or the operator request daemon or service cannot obtain an internal software lock.

**Recommended Action:** Check for the existence and permissions of the lock file itself and the lock file directory: `/usr/openv/volmgr/misc/vmd.lock` (UNIX and

Linux) or *install\_path*\Volmgr\misc\vmd.lock (Windows). Create the directory or folder and adjust the permissions as needed so that vmd can obtain the lock: */usr/opensv/volmgr/misc/vmd.lock* (UNIX and Linux) or *install\_path*\Volmgr\misc\vmd.lock (Windows).

## Media Manager status code 22

**Message:** pool type change is not allowed for <CatalogBackup> pool

**Explanation:** An attempt was made to remove the catalog backup attribute of the default CatalogBackup pool.

**Recommended Action:** Verify that the appropriate pool name was used in this operation.

## Media Manager status code 23

**Message:** database server is down

**Explanation:** A request was made to the EMM server, but the underlying database server does not respond.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- This error can occur if a cold catalog backup is in progress. Retry the request after this operation has completed.

## Media Manager status code 25

**Message:** failed making the database directory

**Explanation:** nbpushdata cannot create a working directory during upgrade.

**Recommended Action:** Determine why the directory */usr/opensv/tmp* (UNIX and Linux) or *install\_path*\tmp (Windows) cannot be created. Check to see what account nbpushdata was run under. Compare it against the security properties of the database folder.

## Media Manager status code 26

**Message:** database open operation failed

**Explanation:** A database file cannot be opened.

**Recommended Action:**

Check for the existence and permissions of the following files in the  
`/usr/opensv/var/global` directory (UNIX and Linux) or  
`install_path\NetBackup\var\global` folder (Windows):

- `external_robotics.txt`
- `external_densities.txt`
- `external_drivetypes.txt`
- `external_mediatypes.txt`

## Media Manager status code 27

**Message:** database read record operation failed

**Explanation:** `nbpushdata` encountered a read error while reading an EMM database record.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- The EMM database may be corrupted. Restore an older EMM database from a saved version or from catalog backups.

## Media Manager status code 28

**Message:** database read operation read too few bytes

**Explanation:** `nbpushdata` encountered a record that was smaller than expected while reading an EMM database record.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- The EMM database may be corrupted. Restore an older EMM database from a saved version or from catalog backups.

## Media Manager status code 32

**Message:** database write record operation failed

**Explanation:** `nbpushdata` encountered an error while writing an EMM database record.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 34

**Message:** media ID not unique in database

**Explanation:** A volume entry being added to or changed in the EMM database had a media ID specified. The specified ID was a duplicate of the media ID for another volume already in the EMM database. All volumes in the EMM database must have a unique media ID.

**Recommended Action:**

- Examine the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- When you add volumes to the EMM database, specify a media ID that is unique.
- If you run `vmphyinv`, there may be two or more media in the tape library with the same media ID.

## Media Manager status code 35

**Message:** volume does not exist in database

**Explanation:** A requested operation encountered a case where a volume query did not return a volume entry that matched the search criteria.

**Recommended Action:**

- Examine the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Ensure that volumes are configured properly on the EMM server that matches the EMM server configured for the robot or set of standalone drives. Use `tpconfig -d` to list the configured EMM server.
- Do the following so the volume query can find a matching volume: update the volume or the device configurations, specify the correct EMM server, modify volume properties, or adjust search criteria.
- If you run `vmphyinv`, none of the media satisfies the search criterion. As such, `vmphyinv` cannot inventory the tape library.

## Media Manager status code 36

**Message:** barcode not unique in database

**Explanation:** A specified barcode in an added or a changed volume entry in the EMM database duplicated a volume barcode already in the database. All volumes in the EMM database must have a unique barcode.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Query or sort volume records by barcode to identify the volume entry with the duplicate barcode.

## Media Manager status code 37

**Message:** robotic volume position is already in use

**Explanation:** A robotic coordinate in an added or a changed volume entry in the EMM database duplicated a volume robotic coordinate in the database. (The robotic coordinate includes the slot number or the slot number and platter side.) All volumes in the EMM database must have unique robotic coordinates.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Query or sort volume records by slot number to identify the volume entry with the duplicate robotic coordinate.

- Change (update or move volume) or delete the existing volume entry if it does not reflect the following: the correct robotic coordinate corresponding to the volume's storage position in the robotic library. If a volume is currently in a drive, the EMM database should still reflect the volume's home slot.

## Media Manager status code 39

**Message:** network protocol error

**Explanation:** An attempt to read data from a socket failed.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the protocol error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the server being connected to is operational.

## Media Manager status code 40

**Message:** unexpected data received

**Explanation:** Message communications (handshaking) was not correct.

**Recommended Action:**

- Verify that the correct version of software is running on all servers.
- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the protocol error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the logs.
- Ensure that no embedded whitespaces exist in the fields that do not allow embedded whitespace.

## Media Manager status code 41

**Message:** invalid media ID for naming mode

**Explanation:** A request to add multiple volumes with a first media ID and a media ID style failed. It fails because the media ID specified was not compatible with the media ID naming style provided.

**Recommended Action:** Provide a first media ID that fits the selected style. For example, the media ID style is two characters and four digits. Then, the least



significant four characters in the first media ID must be digits in the range from 0 to 9. Alternatively, select a media ID style that fits the specified first media ID.

## Media Manager status code 42

**Message:** cannot connect to robotic software daemon

**Explanation:** A connection to a robotic software daemon or process cannot be established. This error can occur when a process tries to connect to the robotic process that is not running. It can also occur if the network or server is heavily loaded and has slow response time.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on.
- Verify that the robotic process to use for robotic control is available  
See "Media and device management components" in the [NetBackup Logging Reference Guide](#).  
If necessary, start the robotic process.
- Ensure that only one configured robot control host exists for each TL8, TLD, and TLH robot. Also ensure that all volumes in the volume configuration have a robot host that matches the configured robot control host.
- Change the volumes or reconfigure the robot in the device configuration as needed.
- Check the system log on the robot control host to see if the robotic process processes the requests when connections to it are attempted.

## Media Manager status code 43

**Message:** failed sending to robotic software daemon

**Explanation:** An attempt to write data to a robotic software daemon or process socket failed.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Identify the robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on. Verify that the robotic process to use for robotic control is available and that it handles requests.
- Identify the robot control host by checking the device configuration. Only one configured robot control host should exist for each TL8, TLD, and TLH robot. All volumes in the volume configuration should have a robot host that matches the configured robot control host.
- Check the system log on the robot control host to see if the robotic process processes the requests when communications with it are attempted.

## Media Manager status code 44

**Message:** failed receiving from robotic software daemon

**Explanation:** An attempt to read data from a robotic software daemon or process socket failed.

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the targeted robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on. Verify that the robotic process to use for robotic control is available and that it handles requests.  
See "Media and device management components" in the [NetBackup Logging Reference Guide](#).
- Identify the robot control host by checking the device configuration. Only one configured robot control host should exist for each TL8, TLD, and TLH robot. All volumes in the volume configuration should have a robot host that matches the configured robot control host.
- Check the system log on the robot control host to see if the robotic process handles requests when communications with it are attempted.  
See "Resolving network communication problems with UNIX clients" in the [NetBackup Troubleshooting Guide](#).  
See "Resolving network communication problems with PC clients" in the [NetBackup Troubleshooting Guide](#).

## Media Manager status code 45

**Message:** failed changing terminal characteristics

**Explanation:** When an attempt was made to change the mode for terminal input between cooked and raw, a system call failed.

**Recommended Action:** Examine the user interface output for the system error that is associated with the failed system call. Then, troubleshoot according to the operating system vendor recommendations.

## Media Manager status code 46

**Message:** unexpected data from robotic software daemon

**Explanation:** Message communications (handshaking) between a process and a robotic software daemon or process failed.

**Recommended Action:**

- Verify that the correct version of software is running on all servers.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the logs.
- Ensure that no embedded whitespaces exist in the fields that do not allow embedded whitespace.
- Check the system log on the robot control host for the errors that the robotic software logged.

## Media Manager status code 47

**Message:** no entries changed

**Explanation:** A requested operation was completed, but no changes to the volume configuration or Media Manager configuration file were made. The administrator may have terminated an operation instead of continuing with proposed changes or the configuration file may already include the configuration entry that was to be added.

**Recommended Action:**

- No action is needed if the administrator aborted the change operation.
- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 48

**Message:** no entries deleted

**Explanation:** A delete volume(s) operation completed. No changes were made to the volume configuration.

**Recommended Action:**

- No action is needed, unless the volumes that were requested to be deleted were not deleted.
- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 49

**Message:** no entries inserted

**Explanation:** An insert volume(s) operation completed. No volumes were added to the volume configuration.

**Recommended Action:**

- No action is needed unless the volumes that were requested to be inserted were not inserted.
- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 50

**Message:** invalid change-entry request

**Explanation:** An invalid request to change volume information was sent to `vmd` on the EMM server.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Check the usage statement for expected usage and compare with the parameters being sent to start the new process.

## Media Manager status code 51

**Message:** cannot auto-eject this robot type

**Explanation:** A request to change volume residence with media eject was sent to `vmd`, but the volume's robot type does not support automated media eject. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the change volume residence requests are not sent to `vmd` on a system that runs an older, incompatible software version level. (The change volume residence requests are requests with eject for the robot type that is involved with a newer release version level.)

## Media Manager status code 52

**Message:** cannot auto-inject this robot type

**Explanation:** A request to change volume residence with media inject was sent to `vmd`, but the volume's robot type does not support automated media inject. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the change volume residence requests are not sent to `vmd` on a system that runs an older, incompatible software version level. (The change volume residence requests are requests with inject for the robot type that is involved with a newer release version level.)

## Media Manager status code 53

**Message:** invalid volume move mode

**Explanation:** A robotic-related request was made that specifies a media movement option that is not supported by all of the affected software components.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the robotic request is sent to a system that runs a release version of the software that supports the particular request.

## Media Manager status code 54

**Message:** robot number and robot type mismatch

**Explanation:** A request was made to add or change volumes in the volume configuration. The robot number to be associated with a volume is already in use. It is associated with another volume in a robot with the same number but of another robot type.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the robot numbers are unique for each physical robot in the EMM database. Delete and re-add a robot. Use a unique robot number if duplicate robot numbers are in use. Use a media management interface to identify the robot numbers that are currently in use for all of the volumes in the volume configuration. If you use a command-line interface, specify the correct robot type for the robot number that is associated with the request.

## Media Manager status code 55

**Message:** robot number and volume group mismatch

**Explanation:** A request was made to add or change the volumes in the volume configuration. The robot number and the volume group that is associated with the volume configuration changes are in conflict with the requirements for volume

groups. All of the volumes in a volume group are required to have the same residence and that includes having the same robot number.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the specified robot number and volume group are compatible. If the volumes in the volume group have a given robot number, then the volumes with a different robot number cannot be added to that volume group. The volumes cannot be moved directly from one robotic volume group to another robotic volume group. The intermediate steps (some volume entries are changed and some are not) would cause a conflict with the robot numbers. Choose a different volume group on the request, or let the volume group be selected automatically. The volume group selection depends on the specific interface being used.

## Media Manager status code 57

**Message:** error auto-generating volume group

**Explanation:** A request was made to add or change the volumes in the volume configuration by using automatic generation of the volume group name. A unique volume group name cannot be generated because all of the available combinations have already been used.

**Recommended Action:** Consolidate the volumes into volume groups within the targeted robot number so that a new volume group can be generated automatically or provide a specific volume group name.

## Media Manager status code 58

**Message:** daemon cannot obtain socket

**Explanation:** `vmd` cannot bind to its socket. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.) When `vmd` attempts to bind to its configured port number, the system call fails. The call fails usually because another process acquired the port before the `vmd` daemon or service started.

**Recommended Action:**

- Examine the daemon debug log for a more detailed message on the system error.

- If another process has the port, use other system commands to determine the process. Based on the result, either change the port number in your services file or map, or terminate the process that has acquired the port.
- UNIX and Linux only: Another possible cause for this error is the use of the `kill` command to terminate `vmd`. To stop `vmd`, the recommended method is to use the command-line request, `vmctrldbm -t`. The use of the `kill` command to stop this process can leave it unable to bind to its assigned port the next time it restarts. When the socket problem occurs, the daemon debug log contains lines similar to the following:

```
unable to obtain bound socket, Address already in use (125)
```

## Media Manager status code 59

**Message:** daemon failed accepting connection

**Explanation:** `vmd` cannot accept a new connection due to a system call failure. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.)

**Recommended Action:**

- Examine the daemon debug log for a more detailed message on the system error. Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Obtain the specific system call failure from the debug log and investigate the operating system functionality that is related to the failure.

## Media Manager status code 60

**Message:** cannot perform operation on this host

**Explanation:** A requested operation is not functional on a particular host.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Initiate the robot inventory update only on the host where the robotic control and drives are configured.



## Media Manager status code 61

**Message:** robot number and robot host mismatch

**Explanation:** A request is made to add or change volumes in the volume configuration or to issue a robot inventory update request. A specified robot host differs from the robot host for other volumes in the same robot (defined as those volumes having the same robot number). All volumes in the EMM database that have a given robot number (for instance, 0) must have the same robot host name.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify the robot host in the device configuration to be the same case-sensitive host name on all hosts where the robot is configured. Re-issue the request. As an alternative, use move-by-volume group to move all of the volumes logically from a robotic volume group to standalone and then back into the robot. Specify the robot host as the host name that is used in the robot configuration. Then, re-issue the request.

## Media Manager status code 62

**Message:** failed redirecting input to pipe

**Explanation:** A system pipe cannot be created.

**Recommended Action:** Check the interface output for the specific system error and investigate the operating system functionality that is related to the failure.

## Media Manager status code 63

**Message:** child process killed by signal

**Explanation:** An unexpected signal terminated a robot inventory update process.

**Recommended Action:** Examine the interface output and debug logs for a more detailed message error. Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 64

**Message:** no child process to wait for

**Explanation:** A media management interface attempted to wait for a child process to complete, but found that no such child process existed.

**Recommended Action:**

- Examine the interface output and debug logs for a more detailed message error. Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation (or try to use a different media management interface) and examine the logs.

## Media Manager status code 65

**Message:** volume group does not exist

**Explanation:** During a request process, the volume group cannot be found within the existing volume entries in the EMM database.

**Recommended Action:**

- Examine the interface output and debug logs for a more detailed message error. Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check for data integrity or consistency problems in the EMM database by using a media management interface. Delete or move the volume entries so that the volume group issues are corrected.

## Media Manager status code 67

**Message:** unable to send exit status

**Explanation:** `vmd` cannot send the status of a requested operation to the requestor. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.)

**Recommended Action:**

- Examine the daemon debug log for a more detailed message on the system error. Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Obtain the specific send or write system call failure from the debug log, and investigate the operating system functionality that is related to the failure.
- Use the following steps to check whether the command or the application interface that sends the request aborts prematurely: enable `reqlib` debug logs, retry the operation, check the debug logs, and observe the application interface output.

## Media Manager status code 68

**Message:** too many volumes in volume group

**Explanation:** A request was made to add or change the volumes in the volume configuration, but the volume number was at its allowable limit. The limit is based on the number of volumes that are allowed in a particular type of robot.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check to see if the volumes are defined in the EMM database. They may be defined in the EMM database that is associated with a slot number zero that may not exist in the robot. Run a robot inventory. Show the contents of the robot report and observe the starting slot number. If the starting slot number is one and a volume is defined in the robot at slot zero, delete the volume entry or move it to a standalone so that the remaining available media slots can be used.

## Media Manager status code 69

**Message:** failed sending request to `vmd`

**Explanation:** A request cannot be sent to `vmd` or to `opr`, even though the initial connection to the server process was successful. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows; `opr` is the operator request daemon or process.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check to see whether the `vmd` or the `opr` process continues to run once it receives the connection from the requestor. Run `netstat -a` or an equivalent

socket diagnostic utility. Check the following to see if the server process is hung up:

- Daemon debug log on the server-side system
- Process status of `vmd` or `opr`

## Media Manager status code 70

**Message:** cannot connect to `vmd` [on host *host name*]

**Explanation:** A process times out while connecting to either `vmd` (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) or to `opr` (the operator request daemon or process). This problem can occur when a connection is attempted and the server process is not running. It also can occur if the network or server is heavily loaded and has a slow response time.

**Recommended Action:**

- On the host where `vmd` is the recipient of the connection, verify that the daemon or the service is running. (The host is the Media Manager host, the Device Host, or the EMM server.) If the daemon or the service is not running, start it. On Windows, `vmd` is the NetBackup Volume Manager service.
- If `vmd` is already running, examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the correct host names are defined in the configuration.
- Check the services file. On UNIX and Linux, verify that the `/etc/services` file (and NIS services if NIS is used) has entries for the `vmd` service. (Note that the `vmd` service always starts `opr`.) On Windows, verify that the `%systemroot%\system32\drivers\etc\services` file has the correct entry for `vmd`. Also verify that the `vmd` port number in the services file agrees with the port number configuration. The port number is noted in the man page for `vmd(1M)`.
- Verify that all of the operating system patches or service packs are installed.
- Ensure that the Media Manager configuration is not tuned so that the load on `vmd` exceeds its ability to service requests. Look for entries in the `vm.conf` file that increase the load. Consider placing the EMM database on a higher performance server and file system if performance is an issue. To reduce the number of volumes in the volume configuration, use inventory filtering for the robot types that support it

- Check the utilities, such as `ipcs -a`, to ensure that the shared memory functions properly. The `oprnd` process may not respond because it cannot attach to shared memory.

## Media Manager status code 71

**Message:** failed sending to `vmd`

**Explanation:** An attempt to write data to a `vmd` socket failed. `vmd` is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the system where `vmd` is running. The system usually is termed the Media Manager host or the EMM server and it defaults to the local system in some user interfaces. Possible causes for the error are a high network load, missing operating system patches or service packs, or an unexpected `vmd` process failure.

## Media Manager status code 72

**Message:** failed receiving from `vmd`

**Explanation:** An attempt to read data from a `vmd` socket failed. `vmd` is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the system where `vmd` is running. The system is usually termed the Media Manager host or the EMM server and it defaults to the local system in some user interfaces. Possible causes for the error are a high network load, missing operating system patches or service packs, or an unexpected `vmd` process failure. Also, the socket read may have failed because the requested operation did not complete within a specified time period. The robotic process

and `vmd` interactions can affect some requests to `vmd`; check the system log for errors on the robotic control host.

## Media Manager status code 73

**Message:** invalid query type

**Explanation:** An invalid volume query request was attempted.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that all Media Manager and user interface binaries are at a compatible version level.

## Media Manager status code 74

**Message:** invalid number of cleanings

**Explanation:** A request was made to change the number of cleanings that remains for one or more volumes in the volume configuration. When the request was made, the specified value was not within the acceptable range. The number of cleanings value may also be invalid in the number of mounts or cleanings field of a barcode rule.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify the number of cleanings value in the range from 0 to 2,147,483,647.

## Media Manager status code 75

**Message:** invalid change type

**Explanation:** An invalid volume change request was attempted.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Verify that all of the Media Manager and user interface binaries are at a compatible version level.

## Media Manager status code 76

**Message:** cannot get host name

**Explanation:** The system call `gethostname(3C)` failed during an attempt to obtain the name of the local host.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Obtain the specific system call failure from the debug log and investigate the operating system functionality that is related to the failure. Run the `hostname` system command to see if the command operates correctly.

## Media Manager status code 78

**Message:** barcode does not exist in database

**Explanation:** A query volume by barcode request did not return a volume entry having the specified barcode, or barcode and media type.

**Recommended Action:**

- Examine the daemon and the `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the volumes are properly configured in the EMM database. Use the `tpconfig -d` command to list the configured EMM server. Select the current server (the one being administered) to be the same as the host, which is the correct EMM server. Do the following so that the volume query can find a matching volume: update the volume or the device configurations, modify the volume properties, or adjust the search criteria as needed. For media in their correct slot locations, run the Rescan or the update barcode request so that the barcode field in the volume configuration matches the actual barcode as interpreted by the robotic library barcode reader.

## Media Manager status code 79

**Message:** specified robot is unknown to `vmd`

**Explanation:** A request was made to query volumes by residence. No volumes were found in the targeted volume configuration that matched the provided robot number, robot type, and robot host.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the volumes are properly configured in the EMM database. Use the `tpconfig -d` command to list the configured EMM server. Select the current server (the one being administered) to be the same as the host, which is the correct EMM server. Perform the following so the volume residence query can find a matching volume: update the volume or the device configurations, modify the volume properties, or adjust the search criteria as needed.

## Media Manager status code 80

**Message:** cannot update database due to existing errors

**Explanation:** The `vmphyinv` command is unable to update the EMM database because of the existing errors. The errors can be as follows:

- A Media Manager volume record belongs to a different robot with the same media ID as the media ID that was read by the tape header.
- The media type, the media GUID, or the volume pool of an assigned volume record needs to be changed.
- A barcode conflict is detected and `vmphyinv` needs to change the barcode of the existing volume record.

**Recommended Action:** The `vmphyinv` command generates a list of errors. Examine the output and resolve all of these errors before you run the utility again.

## Media Manager status code 81

**Message:** robot type and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The robot type and volume group that is associated with the volume configuration changes are in conflict with the requirements for volume groups. All volumes in a volume group are required to have the same



residence, which includes having the same robot type. A requested operation may have tried to associate the special No Volume Group name "---" with a robotic residence.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the specified robot residence and the volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Do not move volumes in the special No Volume Group name to a robotic residence without moving them to a new or auto-generated volume group. Choose a different volume group on the request, or let the volume group be automatically selected. The volume group selection depends on the specific interface being used.

## Media Manager status code 82

**Message:** robot host and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The robot host and volume group that is associated with the volume configuration changes are in conflict with the requirements for volume groups. All volumes in a volume group are required to have the same residence. This residence includes having the same robot host, where robot host equivalence is defined as having the same case-sensitive robot host string.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the specified robot residence and volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Do not try to add volumes for a robot host by using a different form of the robot host name. For example, `acme` is not the same as `acme.veritas.com`. Use the same host name that is used for other volumes in the volume group. If the robot host needs to be changed for volumes in a volume group, do the following: use a single move volume group request (available only in certain media management interfaces) to move the volume group to a standalone residence. Then, move the volume group back to the robotic residence. Specify the robot control host that you want to be associated with the new volume group.

## Media Manager status code 83

**Message:** device management error

**Explanation:** One of the device management errors occurs during the execution of `vmphyinv`.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 84

**Message:** this machine is not the database host

**Explanation:** A request was made to initiate `vmd` on a host other than the local host. `vmd` is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

The `vmd` port numbers other than the default or use of unsupported options can affect the referenced host and port in the interfaces that start `vmd`.

**Recommended Action:**

- Initiate `vmd` on the local host only, by logging on to the host where `vmd` needs to run. Start `vmd` on that host. On UNIX and Linux, run `/usr/opensv/volmgr/bin/vmd [-v]`. On Windows, start the NetBackup Volume Manager service in Services of the system Control Panel.
- If more information is needed to explain the problem, examine the command output, debug logs, and system logs for a more detailed message on the error. See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Make sure that the port numbers are consistent.

## Media Manager status code 85

**Message:** volume daemon fork failed

**Explanation:** A Media Manager daemon or service cannot create a child process due to an error from the system. This error probably is intermittent, based on the availability of resources on the system.

**Recommended Action:**

- Restart the service at a later time and investigate the system problems that limit the number of processes.

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 86

**Message:** failed opening tmp output file

**Explanation:** The `vm.conf` file or temporary working file cannot be opened.

**Recommended Action:** On UNIX and Linux, check for the existence and permissions of the `/usr/opensv/volmgr/misc` directory, `/tmp` directory, and `/usr/opensv/volmgr/vm.conf` file. On Windows, check for the existence and the security properties of the `install_path\Volmgr\vm.conf` file.

## Media Manager status code 87

**Message:** failed redirecting tmp output file

**Explanation:** The system call `dup2(3C)` failed during an attempt to direct interface output from a temporary file to the process's standard output.

**Recommended Action:** Investigate the operating system functionality that is related to the resource limits on the number of open files. Ensure that extraneous signals do not interrupt the processes.

## Media Manager status code 88

**Message:** failed initiating child process

**Explanation:** A command cannot be run. This error can occur due to the following: the command permissions do not allow it to be run or system resources such as memory and swap space are insufficient.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the permissions on the `vmcheckxxx`, `vmupdate`, and `opr` binaries, and (on Windows only) the `rdevmi` installed binary.

## Media Manager status code 89

**Message:** another daemon already exists

**Explanation:** `vmd` (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) tries to initialize and found that it was already running, according to the daemon or the service lock file.

**Recommended Action:** Check to see if `vmd` is already running. Do not try to start another `vmd` daemon or service until you first shut down the daemon or the service that is running. Stop the `vmd` that is running with `vmctrldbm -t`. On Windows, use the system Services interface. If the daemon or the service unexpectedly terminated, remove the lock file. The lock file is `/usr/opensv/volmgr/misc/vmd.lock` (UNIX and Linux) or `install_path\Volmgr\misc\vmd.lock` (Windows). Then, restart `vmd`.

## Media Manager status code 90

**Message:** invalid volume pool

**Explanation:** A request was made to add volumes, change the volume pool for a volume, add a barcode rule, or change a barcode rule. However, the volume pool name or number that is associated with the requested change is in conflict with the requirements for volume pools.

These requirements are as follows:

- Volumes in scratch pools cannot be assigned until they are first moved to another pool.
- Volume pool numbers cannot be negative.
- Volume pool names must consist of from 1 to 20 printable ASCII characters with no embedded whitespace.
- The None volume pool is the only valid pool for the barcode rule entries that specify cleaning a media type.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the specified volume pool does not violate the requirements noted. Use the `vmppool` command to display the pool information. Use the `vmrule` command to display the barcode rule information. Add or change the volume

pools and barcode rules as needed to rectify inconsistencies in cases where the databases are inconsistent or corrupted.

## Media Manager status code 92

**Message:** cannot delete assigned volume

**Explanation:** A delete request was made to a volume and the volume is currently assigned.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Assigned volumes cannot be deleted. If no worthwhile data is on the volume, unassign the media by using the appropriate application interface (it is `bpxupdate` for NetBackup). Then retry the delete volume request.

## Media Manager status code 93

**Message:** volume is already assigned

**Explanation:** A request was made to assign a volume and the volume was already assigned.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Do not try to manually assign any volumes that are already assigned, because it is not valid except for one condition: you can assign volumes for NetBackup catalog backups if the volume is already assigned for NetBackup catalog backups. Always use barcodes that are unique in the six least significant characters across all media in all of the robots, or use media ID generation rules to ensure that unique media IDs are generated in a robot inventory update.

## Media Manager status code 94

**Message:** volume is not in specified pool

**Explanation:** A request was made to assign a volume from a specified volume pool. The volume was in a different volume pool.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- When you assign volumes manually, specify the volume pool that is associated with the volume. Always use barcodes that are unique in the six least significant characters, across all media in all of the robots, or use media ID generation rules to ensure that unique media IDs are generated in a robot inventory update.

## Media Manager status code 95

**Message:** media ID is not the specified media type

**Explanation:** A request was made to assign or add a volume of a specified media type. The volume or physically similar volumes have a different media type.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- When you use the robot inventory update to make changes to the volume configuration, do the following: ensure that all of the volumes of the same physical cartridge type (for example, 3590J in TLH robots) map to a single media type, such as HCART. This check ensures that all of the media in the robotic library can be mounted on drives with a compatible drive type.
- When you assign the volumes manually, specify the media type that is associated with the volume. Always use barcodes that are unique with respect to the six least significant characters, across all of the media in all of the robots. You can also use media ID generation rules to ensure that the unique media IDs are generated when you use the robot inventory update.

## Media Manager status code 96

**Message:** oprd returned abnormal status

**Explanation:** A request that the `oprd` services (the operator request daemon or process) returned an abnormal status.

**Recommended Action:**

- On Windows, when you auto-configure devices or initiate the NetBackup Device Manager service from a graphical or a command line interface, ensure that the service is not disabled in the system services configuration.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- In general, any device management-related errors that occur on a particular host accompany the operator request daemon or process and remote device management errors. Check for errors in the debug and the system or the application logs on the host where `opr`d was started or where it is running. The host is often a targeted device host or scan host.

The kinds of failed requests that `opr`d services can include the following:

- Down, up, or reset drives
- Change drive comments
- Deny or resubmit mount requests
- Assign drives
- Start or stop `ltid`
- Obtain `ltid` status
- Display drive status
- Manage pending actions
- Set NDMP attributes
- Configure devices
- Clean drives
- Obtain host version and device configuration information
- Scan shared drives

## Media Manager status code 97

**Message:** rule does not exist in rule database

**Explanation:** A request was made to change or delete a barcode rule, but the barcode rule with the specified barcode tag cannot be found.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- List the configured barcode rules in the EMM database. Adjust the barcode tag that is specified on the change request, the delete request, or the targeted host. Then, the barcode rule is found when the request is retried.

## Media Manager status code 101

**Message:** media type and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The media type and volume group that are associated with the volume configuration changes are in conflict with the requirements for the volume groups. All of the volumes in a volume group are required to have the same residence that also includes having the same media type. The media types that are used for data and their associated cleaning media types are considered to be the same with regard to volume group restrictions.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the specified media type and volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Choose a different volume group on the request, or let the volume group be automatically selected. The volume group selection depends on the interface that is being used.

## Media Manager status code 102

**Message:** invalid pool database entry

**Explanation:** The volume pool database is corrupt. It contains some records that are not compatible with the installed product binaries.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.



See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Use `vmppool` to investigate the integrity of the volume pool database. The daemon debug log file should indicate the expected number of fields and the found number of fields in the pool record. Restore a saved version of the pool database if the pool database cannot be manually corrected.

## Media Manager status code 104

**Message:** failed appending to pool database

**Explanation:** A request was made to add, change, or delete a volume pool in the volume pool configuration, but the pool record cannot be appended to the volume pool database file.

**Recommended Action:**

- Examine the daemon debug log for a more detailed message on the system error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Examine the permissions and the available file system space for writing to the database as follows:
  - On UNIX and Linux: `/usr/opensv/volmgr/database/poolDB`
  - On Windows: `install_path\Volmgr\database\poolDB`

## Media Manager status code 105

**Message:** poolname is not unique in pool database

**Explanation:** A request was made to add a volume pool in the volume pool configuration. The pool name that is specified is a duplicate of the name for an existing volume pool.

**Recommended Action:** On the add volume pool request, specify a volume pool name that is not already in use on the targeted EMM database host.

## Media Manager status code 109

**Message:** pool does not exist in pool database

**Explanation:** A requested operation encountered a case where the specified volume pool was not found in the volume pool configuration. The requests that can return this error code are as follows:

- Add, change, delete, or query volume pool
- Add or change barcode rule
- Add or change volume
- Query scratch volumes
- Robot inventory report or update

**Recommended Action:**

- Examine the daemon and the `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the volumes are properly configured on the EMM server. Use the `tpconfig -d` command to list the configured EMM server. Select the current server (the one being administered) to be the same as the host that is the correct EMM server for a targeted device.
- Do the following so that the requested operation can find the requested volume pool: update the volume or the device configurations, modify the volume properties, or adjust the search criteria as needed. Investigate the inconsistencies between the EMM database and the volume pool database, and restore or correct those databases from a previous state, as needed.

## Media Manager status code 110

**Message:** pool is in use

**Explanation:** The operation on a media pool failed because the media pool is in use.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the integrity of the file system and volume pool database as follows:
  - On UNIX and Linux: `/usr/openv/volmgr/database/poolDB`
  - On Windows: `install_path\Volmgr\database\poolDB`
- Make sure that the media pool is not in use by some other table like barcode rule.

## Media Manager status code 111

**Message:** the specified pool is not empty

**Explanation:** A request was made to delete a volume pool. Either the volume pool was not empty, or it could not be determined whether or not the volumes were still associated with the specified volume pool.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use a media management interface to query for the volumes that are associated with the pool specified for deletion. Ensure that all of the volumes in a volume pool are associated again with another pool before trying to delete the volume pool. Use the change volume operations to change the volume pool for a volume.

## Media Manager status code 112

**Message:** no pools in the pool list

**Explanation:** Unexpectedly, the volume pool list is empty.

**Recommended Action:** The volume pool list should contain a minimum of the following four pools: None, NetBackup, Catalog Backup, and DataStore. Investigate the integrity of the EMM database. Restore the EMM database from catalog backups.

## Media Manager status code 113

**Message:** invalid expiration date

**Explanation:** A request was made to change the media expiration for one or more volumes in the volume configuration, but the date specified was not valid.

**Recommended Action:**

When you change the media expiration, provide the date in the format specified by the media management interface documentation.

## Media Manager status code 114

**Message:** invalid maximum mounts

**Explanation:** A request was made to change the limit for the number of times a volume can be mounted with write access for one or more volumes in the volume configuration. The specified value is not within the acceptable range. The maximum

number of mounts value may also be invalid in the number of mounts or cleanings field of a barcode rule.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a maximum mounts value in the range from 0 to 2,147,483,647.

## Media Manager status code 115

**Message:** volume has passed expiration date

**Explanation:** A request was made to assign a volume and the volume expiration date has expired in relation to the current system date.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Extend the active life of the physical media: change the volume expiration date to a future date in relation to the current system date or time. Alternatively, replace the media with the other media that still contains useful life. Check the system date and time and reset it as needed.

## Media Manager status code 116

**Message:** volume has exceeded maximum mounts

**Explanation:** A request was made to assign a volume. The volume's number of mounts exceeds the maximum number of mounts allowed for the volume.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Extend the active life of the physical media by increasing the volume's maximum number of mounts or setting the maximum number of mounts to infinite. Alternatively, replace the media with other media that still contains useful life.

## Media Manager status code 117

**Message:** operation not allowed on cleaning cartridge

**Explanation:** A request was made to change a volume's expiration or maximum number of mounts. The operation is not allowed because the volume is a cleaning cartridge.

**Recommended Action:**

- If the volume is a cleaning cartridge, perform a valid operation such as changing the number of cleanings that remain for the cleaning cartridge.
- If the volume's media type cannot be determined, examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- If the targeted volume is incorrectly configured as a cleaning tape, delete the cleaning volume. Then, update the volume configuration using options to define a new volume with the appropriate media type.

## Media Manager status code 118

**Message:** cannot delete one of the default volume pools

**Explanation:** An attempt was made to delete one of the special, predefined volume pools. The None, NetBackup, Catalog Backup, and DataStore volume pools are fixed volume pools in the volume pool configuration and cannot be deleted.

**Recommended Action:** Do not attempt to delete the None, NetBackup, Catalog Backup, and DataStore volume pools.

## Media Manager status code 119

**Message:** invalid rule database entry

**Explanation:** The barcode rule database is corrupt. It contains records that are not compatible with the installed product binaries.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use `vmrule` to investigate the integrity of the barcode rule database. The daemon debug log file should indicate the number of expected fields and the number of

found fields in the barcode rule record. Restore a saved version of the barcode rule database if the barcode rule database cannot be manually corrected.

## Media Manager status code 121

**Message:** failed appending to rule database

**Explanation:** A request was made to add, change, or delete a barcode rule. A barcode rule record cannot be appended to the barcode rule database file.

**Recommended Action:** Examine the daemon debug log for a more detailed message on the system error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 122

**Message:** barcode tag is not unique in rule database

**Explanation:** A request was made to add a barcode rule. The specified barcode tag was a duplicate of the tag for an existing barcode rule.

**Recommended Action:** On the add barcode rule request, specify a barcode tag that is not already in use.

## Media Manager status code 126

**Message:** not authorized to connect to `vmd`

**Explanation:** A caller requesting services from `vmd` is either not authenticated or not authorized, or a problem is encountered when two systems attempt to authenticate one another.

**Recommended Action:**

- See the [NetBackup Security and Encryption Guide](#) for information on `vmd` security.  
`vmd` security is based on NetBackup authentication or authorization and the media server entries defined in `bp.conf/Host Properties` on the master server for the specific NBU domain.
- Examine the debug log files for a more detailed message on the authentication or the authorization problem.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Correct the `vmd` security configuration by modifying the authentication configuration.

---

**Note:** Ensure that both the source and the destination machines are within a single NBU domain.

---

- If an authentication problem (rather than a configuration issue) is suspected, do the following:
  - Check the `methods_allow.txt` files on the systems that have problems to ensure that authentication is enabled. The files are in the following locations:  
On Windows: `install_path\NetBackup\var\auth`  
On UNIX and Linux: `/usr/opensv/var/auth`
  - On the systems that have the authentication problem, remove the remote host that is not authenticated from the `methods_allow.txt` file.  
For example, if Host A and Host B have the problem, remove Host A from the file on Host B, and vice versa.  
Retry the operation. If the problem still exists, the connection problems are not related to authentication.
  - Add back the removed hosts and retry the operation.

## Media Manager status code 127

**Message:** unable to generate a unique media ID

**Explanation:** A request was made to add volumes in the volume configuration by using the robot inventory update or by using a media ID seed. A unique media ID was not generated because the "use seed" option was not specified, or because the available media ID combinations were used up.

**Recommended Action:** If you use robot inventory update, either ensure that all of the media in the robotic library have readable barcode labels, or request updates by using a seed to generate media IDs for non-barcoded media automatically. If the volumes are added by specifying a seed, use a seed that allows media ID character combinations beyond those already in use. To identify the slot that is associated with the media that may not have a readable barcode, examine the command output.

## Media Manager status code 129

**Message:** invalid drive name

**Explanation:** A request was made to the EMM/DA for a shared drive, and the drive name was not recognized.

**Recommended Action:**

- Examine the daemon and the `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the drive name is from 1 to 48 ASCII characters in length. The following special characters are allowed: period (.), plus (+), minus (-), and underscore (\_).
- Verify that the correct version of software is running on all of the servers.

## Media Manager status code 130

**Message:** requested drive is already reserved

**Explanation:** A request was made to reserve a shared drive with the EMM/DA, but the drive was already reserved for another host.

This error is a normal occurrence when the drive resources are oversubscribed for either of the following reasons:

- Independent schedulers or applications access the same pool of drives
- Hardware or media errors cause some drives that are allocated to jobs to become unavailable.

**Recommended Action:**

- Check the system log and the application (`bptm`) debug log to determine if hardware or media errors have caused the drives to become unavailable.
- If more information is needed on the drive reservation problem, examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 131

**Message:** requested drive is not registered for host

**Explanation:** A request was made to reserve a shared drive with the EMM server. The requesting host did not register the drive, although that host had registered other drives.



This abnormal condition can occur when two different hosts with the same name registered different drive lists with the EMM server and one of those hosts requested a drive reservation. (The same host name occurs when the `SSO_HOST_NAME` entries in the `vm.conf` file override the local host name.)

**Recommended Action:** Use unique (non-duplicate) strings for host names and the `SSO_HOST_NAME` configuration file entries.

## Media Manager status code 132

**Message:** requested drive is not currently registered

**Explanation:** A request was made to reserve or release a shared drive with the EMM server. The requesting host or any other host has not registered the drive.

**Recommended Action:** This condition is abnormal. It can occur when the EMM server was stopped and restarted. This situation is automatically handled because the requesting host re-registers its drives with the EMM server when this error is encountered.

## Media Manager status code 133

**Message:** requested drive is not reserved by host

**Explanation:** A request was made to release a shared drive with the EMM server. The requesting host did not reserve the drive, although it was reserved for another host.

This condition is abnormal. It can occur if a network problem or a suspended process exists, as in the following examples:

- Host A reserves a shared drive.
- Host A becomes unavailable for some time and is unable to communicate with other hosts.
- Host B determines that the host having the reservation (Host A) is no longer available. Host B then makes a request to the EMM/DA denoting Host A as unavailable.
- Another host (such as Host A or Host C) reserves the drive.
- The host that originally owned the drive reservation tries to release the drive.

**Recommended Action:** Correct the network or the process problem that led to the communications problem. Ensure that unique non-duplicate strings are used for host names and for the `SSO_HOST_NAME` configuration file entries.

## Media Manager status code 134

**Message:** requested drive is not currently reserved

**Explanation:** A request was made to the EMM/DA to release a shared drive, but none of the hosts reserved the drive.

This condition is abnormal. It can occur if there a network problem or a suspended process exists, as in the following examples:

- Host A reserves a shared drive.
- Host A becomes unavailable for some time and is unable to communicate with other hosts.
- Host B determines that the host having the reservation (Host A) is no longer available. Host B then makes a request to the EMM/DA denoting Host A as unavailable.
- The host that originally owned the drive reservation tries to release the drive.

**Recommended Action:** Correct the network or the process problem that led to the communications problem. Ensure that unique non-duplicate strings are used for host names and for the `SSO_HOST_NAME` configuration file entries.

## Media Manager status code 135

**Message:** requested host is not currently registered

**Explanation:** A request was made to the EMM/DA to reserve or release a shared drive or designate a host as unavailable. The host (that reserved or released the drive or that was designated as unavailable) was not registered with the EMM/DA.

This condition is abnormal and can occur in the following situations:

- The EMM server was stopped and restarted. This situation is automatically handled, because the requesting host re-registers its drives with the EMM server when this error is encountered.
- A host was unregistered with the EMM server and another host declared the host to be unavailable.

**Recommended Action:** If the host was declared as unavailable, determine whether it should be available. Correct the underlying network problems or restart `ltid` (the device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).

## Media Manager status code 136

**Message:** invalid host name

**Explanation:** A device host was added to the Media Manager configuration, or a request was made to the EMM server and the host name exceeded the allowable length.

**Recommended Action:** Limit the host names to 256 ASCII characters or less.

## Media Manager status code 137

**Message:** oprd request is not supported on the remote host

**Explanation:** An invalid request was sent to the operator request process.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the targeted host. Verify that all of the Media Manager binaries on that host are at a compatible version level with the other hosts that are part of the configuration. Update the software version as needed.

## Media Manager status code 138

**Message:** media generation rule already exists

**Explanation:** You or a NetBackup media management interface attempted to add a `MEDIA_ID_BARCODE_CHARS` rule that already exists. The same rule cannot be added twice.

**Recommended Action:** Examine the listing of the `MEDIA_ID_BARCODE_CHARS` rules again.

The description of the `MEDIA_ID_BARCODE_CHARS` rules is available at the following location:

See "About the vm.conf configuration file" in the [NetBackup Administrator's Guide, Volume II](#).

## Media Manager status code 139

**Message:** media generation rule does not exist

**Explanation:** You or a NetBackup media management interface attempted to delete a `MEDIA_ID_BARCODE_CHARS` rule that does not exist.

**Recommended Action:** Examine a listing of the `MEDIA_ID_BARCODE_CHARS` rules again.

The description of the `MEDIA_ID_BARCODE_CHARS` rules is available at the following location:

See "About the `vm.conf` configuration file" in the [NetBackup Administrator's Guide, Volume II](#).

## Media Manager status code 140

**Message:** invalid media generation rule

**Explanation:** You or a NetBackup media management interface attempted to add an incorrect `MEDIA_ID_BARCODE_CHARS` rule.

**Recommended Action:** Ensure that the `MEDIA_ID_BARCODE_CHARS` rule is composed correctly.

The description of the `MEDIA_ID_BARCODE_CHARS` rules is available at the following location:

See "About the `vm.conf` configuration file" in the [NetBackup Administrator's Guide, Volume II](#).

## Media Manager status code 141

**Message:** invalid number of mounts

**Explanation:** A request was made to change the number of times that a volume was mounted, and the value specified was not within the acceptable range.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a number of mounts value in the range from 0 to 2,147,483,647.

## Media Manager status code 142

**Message:** invalid off-site location

**Explanation:** The off-site location for a volume exceeds 25 ASCII characters in length or it contains unprintable characters.

**Recommended Action:** When you add or change a volume record, ensure the following: the off-site location field contains only printable characters and does not exceed 25 ASCII characters in length.

## Media Manager status code 143

**Message:** invalid off-site sent date

**Explanation:** A request was made to change the off-site sent date for one or more volumes in the volume configuration, but the date specified was invalid.

**Recommended Action:** When you change the off-site sent date, provide the date in the format specified by the Media Management interface documentation.

## Media Manager status code 144

**Message:** invalid off-site return date

**Explanation:** A request was made to change the off-site return date for one or more volumes in the volume configuration, but the date specified was invalid.

**Recommended Action:** When you change the off-site return date, provide the date in the format specified by the Media Management interface documentation.

## Media Manager status code 145

**Message:** requested drive is already reserved by host

**Explanation:** A request was made to the EMM/DA to reserve a shared drive. The drive was already reserved for the requesting host.

This condition is abnormal. It can occur if two different hosts with the same name registered the same drive name with the EMM/DA. (The same host name occurs when the `SSO_HOST_NAME` entries in the `vm.conf` file override the local host name.) In this case, one of those hosts has a drive reservation and the other host tries to reserve the same drive.

**Recommended Action:** Use unique non-duplicate strings for host names and for the `SSO_HOST_NAME` configuration file entries.

## Media Manager status code 146

**Message:** incompatible database version

**Explanation:** A requesting process or `vmd` encountered an invalid or an unknown database or communications protocol. The possible datastores that an error affects are volume, volume pool, barcode rule, global device database, and shared drive information.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Identify the target components (for example, `vmd` and daemons or services, or user interfaces on local or remote hosts). Verify that all of the Media Manager binaries are at a compatible version level. Depending on which requests encountered the invalid version, determine whether or not the database is corrupt. Use an appropriate interface to query for the type of information that is involved in the error condition.

## Media Manager status code 147

**Message:** invalid off-site slot

**Explanation:** A request was made to change the off-site slot location for a volume and the value specified was not within the acceptable range.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify an off-site slot value in the range from 0 to 2,147,483,647.

## Media Manager status code 148

**Message:** invalid off-site session ID

**Explanation:** A request was made to change the off-site session ID for a volume and the value specified was not within the acceptable range.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify an off-site session ID in the range from 0 to 2,147,483,647.

## Media Manager status code 149

**Message:** current version does not support this configuration

**Explanation:** A request cannot be performed because it attempted to reference unlicensed functionality. For example, a request to add a volume with a media type that is not valid for the licensed product.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- List the license keys that were installed and verify that the referenced functionality is supported with the currently installed license keys. Check to see that the databases that define externalized object types are in place and not corrupted. These database files are the following, in the `/usr/opensv/var/global` directory (UNIX and Linux) or `install_path\NetBackup\var\global` folder (Windows):
  - `external_densities.txt`
  - `external_drivetypes.txt`
  - `external_mediatypes.txt`
  - `external_robotics .txt`

## Media Manager status code 150

**Message:** registering this host would exceed the maximum allowed

**Explanation:** The EMM/DA received a request to register the shared drives from a host that was not currently registered. The maximum number of hosts that are registered with this EMM/DA were already reached. The current limit for the number of hosts that can register with the EMM/DA is 255.

**Recommended Action:**

- Restrict the size of the SSO configuration to no more than 255 hosts.
- Break up the media and the device management domain into multiple domains, with all of the domains having 255 or fewer hosts that register the shared drives.

## Media Manager status code 152

**Message:** global device database record not found

**Explanation:** A request was made to update a global device database record and the record specified was not found in the global device database. This condition can occur when a device configuration change is made after the global device database host has changed.

**Recommended Action:** If the request to update the record fails because the record does not exist, a request is made to add the missing record. No action is required.

## Media Manager status code 153

**Message:** device entry is not unique in global device database

**Explanation:** A request was made to add a global device database record and the record specified was a duplicate of an existing record. This condition can occur if two processes simultaneously update the device configuration on the same host.

**Recommended Action:**

- Coordinate the changes to the device configuration so that the changes come from a single source.
- Investigate the global device database changes on the server (database) side by examining the daemon debug log file for a more detailed error message. See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 155

**Message:** global device database append operation failed

**Explanation:** A request was made to change the device configuration and a global device database record cannot be written to the global device database file.

**Recommended Action:**

Examine the daemon debug log for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 160

**Message:** the global device database device type is invalid

**Explanation:** An invalid device type appears in a request to modify the device configuration.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error. See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the targeted host. Verify that all of the Media Manager binaries on that host are at a compatible version level with the other hosts that are part of the configuration. Update the software version as needed.



## Media Manager status code 162

**Message:** the global device database device name is invalid

**Explanation:** An invalid or a missing device name was encountered in a request to modify the device configuration.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Identify the targeted host. Verify that all of the Media Manager binaries on that host are at a compatible version level with the other hosts that are part of the configuration. Update the software version as needed.

## Media Manager status code 163

**Message:** the operation requested has failed

**Explanation:** The requested operation failed. The reason was not specified.

**Recommended Action:** This error code may appear for a number of reasons. Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 164

**Message:** the robotic daemon returned an invalid volume GUID

**Explanation:** An invalid RSM GUID was returned from the RSM API. (RSM is the Microsoft Removable Storage Manager. GUID is a Global Unique Identifier.)

**Recommended Action:**

- Examine the system's application log, the Removable Storage system interface, and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the logs. From the daemon debug log file, determine the media ID that has the invalid RSM GUID.
- Make sure that the software components are compatible.

## Media Manager status code 165

**Message:** Evaluation period expired. Go to [www.veritas.com](http://www.veritas.com) to order this product.

**Explanation:** The NetBackup evaluation software has expired.

See the address in the message or [www.veritas.com/enterprise/](http://www.veritas.com/enterprise/) for ordering information.

**Recommended Action:** Obtain a licensed copy of NetBackup.

## Media Manager status code 166

**Message:** media access port not available

**Explanation:** A request was made to physically move a volume into or out of a robotic library, but the media access port was unavailable.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that the move request was not sent to a robotic control daemon or process on a system that runs an older, incompatible software version.
- Ensure that the targeted robotic control daemon or process operates normally.

## Media Manager status code 167

**Message:** ADAMM GUID is not unique in the database

**Explanation:** A volume entry that was added to or changed in the EMM database had a specified ADAMM GUID. It was a duplicate of the ADAMM GUID for another volume already in the EMM database. All of the volumes in the EMM database must have an ADAMM GUID that is either unique or null. (ADAMM is Advanced Device and Media Management, and GUID is a Global Unique Identifier.)

**Recommended Action:**

- Examine the command output (if available) and the daemon and `reqlib` debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- From the daemon debug log file, determine the volume that has an ADAMM GUID conflict with the volume entry that is added or changed.

## Media Manager status code 168

**Message:** ADAMM GUID does not exist in database

**Explanation:** The EMM database was queried for a specified ADAMM (Advanced Device and Media Management) GUID, and no volumes were found that matched the specified criteria. (The GUID is a Global Unique Identifier.)

**Recommended Action:** Run `vmphyinv` for the media whose ADAMM GUID does not exist in the database.

## Media Manager status code 169

**Message:** internal database access failure

**Explanation:** During an update of a drive status from a pre-7.7 NetBackup server in EMM, a problem occurred.

**Recommended Action:** The actions are as follows:

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

## Media Manager status code 171

**Message:** a scratch pool is already defined

**Explanation:** A new scratch pool cannot be defined because another scratch pool already exists.

**Recommended Action:** Use the scratch pool that is already defined or delete the current scratch pool and create a new scratch pool.

## Media Manager status code 172

**Message:** pool not defined as a scratch pool

**Explanation:** You or a NetBackup media management interface have tried to delete (unset) a scratch pool that is not defined as a scratch pool.

**Recommended Action:** To delete the scratch pool, use the `vmppool` command. Ensure that the name of the pool that is specified with the `unset_scratch` option is the correct name of the scratch pool.

## Media Manager status code 173

**Message:** invalid scratch pool name

**Explanation:** You or a NetBackup media management interface have tried to specify the NetBackup, DataStore, or None pool as a scratch pool. The NetBackup, DataStore, and None pools cannot be specified as scratch pools.

**Recommended Action:** Create a scratch pool with a different name.

## Media Manager status code 175

**Message:** unable to open the device test state file

**Explanation:** The process is not able to open the state file, mostly likely because another process locked it.

**Recommended Action:** Try again to open the state file. If you cannot open the state file, you may have to remove the file, which will result in a loss of the previous test runs.

## Media Manager status code 176

**Message:** unable to find any records in the device test database

**Explanation:** The state file exists, but it is empty. This error indicates that no previous test runs have occurred.

**Recommended Action:** None required.

## Media Manager status code 177

**Message:** request can only be performed on the Media and Device Management Domain Server

**Explanation:** The host that this request was performed on is blocked from being a database host. An administrator blocked the host to restrict which hosts are allowed to be EMM servers.

**Recommended Action:**

- Verify that you specified the correct EMM server (the `-h` option on the command line). If you did not specify the database host, the command line defaults to the local host, while the console uses the currently administered host.
- Contact the administrator in charge of this configuration and verify that the host was intentionally blocked from being a database host. If not, remove the `NOT_DATABASE_HOST` flag in the host's `vm.conf` file. To do this without having to stop and restart the daemons, use the following command:

```
vmquery -h <hostname> -remove_not_db_host.
```

To add this entry to a host without having to stop and restart the daemons, use the following command: `vmquery -h <hostname> -add_not_db_host.`

## Media Manager status code 181

**Message:** not authorized to connect to robotic daemon

**Explanation:** A caller requesting services from a robotic daemon is not authenticated or authorized, or a problem occurs when two systems try to authenticate one another.

**Recommended Action:**

- See the [NetBackup Security and Encryption Guide](#) for information on Media Manager security.  
Media Manager security is based on NetBackup authentication or authorization and the media server entries defined in `bp.conf/Host Properties` on the master server for the specific NBU domain.
- Examine the debug log files for a more detailed message on the authentication and authorization problem.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Determine whether the authorization fails on `vmd`. Examine the debug log files for Media Manager status code 126 occurrences (not authorized to connect to `vmd`).
- Correct the Media Manager security configuration by modifying the authentication configuration and the `ENABLE_ROBOT_AUTH` entry.

---

**Note:** Ensure that both the source and the destination machines are within a single NBU domain.

---

- If an authentication problem (rather than a configuration issue) is suspected, do the following:
  - Check the `methods_allow.txt` files on the systems that have problems to ensure that authentication is enabled. The files are in the following locations:  
On Windows: `install_path\NetBackup\var\auth`  
On UNIX and Linux: `/usr/opensv/var/auth`
  - On the systems that have the authentication problem, remove the remote host that is not authenticated from the `methods_allow.txt` file and retry the operation.

For example, if Host A and Host B have the problem, remove Host A from the file on Host B, and vice versa.

If the problem still exists, the error is caused by connection problems that are not related to the authentication.

Add the removed names and retry the operation.

## Media Manager status code 182

**Message:** device test state file does not exist

**Explanation:** The state file does not exist. The reason may be because no tests have been run yet.

**Recommended Action:** If the state file is lost, any previous test runs are also lost. The recommended action is to start again.

## Media Manager status code 185

**Message:** the robotic library is full and may still have media in its map

**Explanation:** During a robot inventory update, the user attempted to use the `empty_map` option. The MAP contained more media than the space allowed in the library. In this case, the inventory update was successful, but the `empty_map` part was only partially successful. Those media that are still in the MAP are not changed or added in the EMM database.

**Recommended Action:** No action is necessary on the user's part except to be aware that not all of the media was removed from the MAP and placed into the library.

## Media Manager status code 186

**Message:** invalid container ID

**Explanation:** A NetBackup Vault container ID was used with an invalid character.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation with a container ID that does not contain invalid characters.

## Media Manager status code 187

**Message:** VxSS authentication failed

**Explanation:** The parties on either end of a socket connection cannot mutually authenticate each other.

**Recommended Action:**

- Ensure that the Veritas Product Authentication Service is installed and configured. For complete installation instructions, see the [NetBackup Security and Encryption Guide](#).
- Check that both parties have a valid certificate by examining the listed expiry date from the `bpnbat -WhoAmI` command. For example:

```
bpnbat -WhoAmI
Name: JDOG
Domain: MYCOMPANY
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
Expiry Date: Sep 19 12:51:55 2009 GMT
Authentication method: Microsoft Windows
Operation completed successfully.
```

- Shows an expiry date of September 19th, 2009. After 12:51:55 GMT, this credential is no longer valid and a new credential is required.
- If you run from the **NetBackup Administration Console**, close and reopen the console. The console automatically obtains a credential for the currently logged in identity, if possible. By default, these certificates are valid for 24 hours. The following is an example of how to extend the credential beyond 24 hours to 30 days (2592000 seconds):
- ```
# vssat setexpiryintervals -p <plugin_name> -t <user> -e 2592000
```
- Ensure that the certificates for both sides either use the same broker, are children of the same root broker, or have trusts established between them. More information is available on broker hierarchies and how to establish trust relationships between brokers. See the [NetBackup Security and Encryption Guide](#).
- Ensure that connectivity is possible between the physical systems in question. If general sockets cannot connect between the machines (such as `ping` and `telnet`), network issues unrelated to NetBackup may be the cause of this problem.
- Ensure that the system has sufficient swap space and that the following directories are not full:

- /home/username
- /usr/opensv/netbackup/logs
- /tmp

## Media Manager status code 188

**Message:** VxSS Access Denied

**Explanation:** The user identity that is used to attempt an operation does not have the permissions needed to perform the action.

**Recommended Action:**

- If you use the default groups, make certain that the user attempts to perform an operation appropriate for that group. For example, a member of NBU\_Operators is unable to modify policy information because it is a permission that is reserved for administrator roles.
- Ensure that the system has sufficient swap space and that the following directories are not full:
  - /home/username
  - /usr/opensv/netbackup/logs
  - /tmp
- If you use your own defined groups and permissions, first determine the object with which the operation is associated. Then, add the permissions relative to the action. For example, a user is required to up and down drives but does not currently have permission to do so. Verify that the user belongs to the correct authorization group.

If necessary, verify that the group has Up and Down permissions on the Drive object within the **Group Permission** tab. If necessary, you can increase the verbosity level of NetBackup to locate what object and what permissions are required for the failing request. The pertinent lines in the debug logs look similar to the following:

```
17:19:27.653 [904.872] <2> GetAzinfo: Peer Cred Info.  
Name: JMIZZLE  
Domain: MYCOMPANY  
Expiry: Sep 24 21:45:32 2003 GMT  
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx  
AuthType: 1  
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5082:  
Function: VssAzAuthorize. Object  
NBU_RES_Drives
```



```
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5083:  
Function: VssAzAuthorize. Permissions Up  
17:19:40.171 [904.872] <2> VssAzAuthorize: vss_az.cpp.5166:  
Function: VssAzAuthorize. 20 Permission denied.
```

In the example, the user JMIZZLE attempts to perform an operation that requires the Up permission on the Drives object. To diagnose the problem, examine the group(s) to which the user belongs to ensure that the appropriate group includes the Up permission. (Up is a member of the Operate permission set for Drives.)

## Media Manager status code 189

**Message:** failed to initialize a connection to the Enterprise Media Manager

**Explanation:** A request to initialize a connection with the EMM server failed or was already initialized.

**Recommended Action:**

- Verify that `pbx_exchange` and `nbemm` are running.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

## Media Manager status code 190

**Message:** the request sent to the Device Allocator has failed

**Explanation:** A request to reserve or release a drive with the DA (EMM server) failed.

**Recommended Action:**

- Verify that `pbx_exchange` and `nbemm` are running.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

- For a DA reserve drive request, verify that another host has not already reserved the drive.
- For a DA release drive request, verify that the drive is DA reserved by the host requesting the DA release and has not already been released.

## Media Manager status code 191

**Message:** invalid EMM argument

**Explanation:** An invalid argument was provided on a call to the EMM server.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 192

**Message:** unknown EMM error code

**Explanation:** An unknown error was returned from the EMM server.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 193

**Message:** generic EMM SQL error

**Explanation:** The EMM server received an error from the underlying database.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Media Manager status code 194

**Message:** EMM DB record not found

**Explanation:** During a NetBackup upgrade a prerequisite host was not upgraded in the correct order.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the proper upgrade order is followed as described in the [NetBackup Installation Guide](#).

## Media Manager status code 195

**Message:** CORBA communication error

**Explanation:** While trying to communicate with the EMM server, a problem occurred.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the Veritas Private Branch Exchange (VxPBX) processes new requests.
- Verify that the EMM server processes new requests.

## Media Manager status code 196

**Message:** EMM database error

**Explanation:** The calling program does not recognize the error the EMM server returned.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the EMM server processes new requests.

## Media Manager status code 198

**Message:** pool not defined as a catalog backup pool

**Explanation:** An attempt was made to remove the Catalog Backup attribute from a pool in which it was not set.

**Recommended Action:** Verify that the appropriate pool name was used in this operation.

## Media Manager status code 199

**Message:** the media is allocated for use

**Explanation:** A request was made to modify a media that was in use.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation once the media is no longer in use.

# Device configuration status codes

This chapter includes the following topics:

- [Device configuration status codes](#)

## Device configuration status codes

Device configuration status codes appear in exit status and command output for the `tpconfig` and the `tpautoconf` commands, and in system or debug logs. The programs that call `tpconfig` and `tpautoconf`, such as media and device management user interfaces and the `vmopr cmd` command, also present these codes.

### Device configuration status code 0

**Message:** Success

**Explanation:** A requested operation was successfully completed.

**Recommended Action:** None

### Device configuration status code 1

**Message:** Cannot execute command, permission denied

**Explanation:** Either a user or process that did not have root privileges (on UNIX and Linux) or administrator privileges (on Windows) started the process, or the EMM server name cannot be set.

**Recommended Action:**

- If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX and Linux) and reissue the device configuration request.
- Establish a common EMM server name as follows:
  - Run `tpautoconf -get_gdbhost` on other hosts.
  - Set the EMM server name with

```
tpautoconf -set_gdbhost host_name
```

where *host\_name* is the host name returned by `tpautoconf -get_gdbhost`.

## Device configuration status code 2

**Message:** The device\_mappings file has invalid license info

**Explanation:**

The problem concerns one of the following files:

`/usr/opensv/share/device_mappings.txt` (UNIX and Linux) or

`install_path\VERITAS\NetBackup\share\device_mappings.txt` (Windows).

- The file does not exist.
- The file is for a different version of NetBackup. You can find out what version it is by reading the header in the file.
- The file has a corrupted licensing digest.

**Recommended Action:** Download the latest device mapping file from the following Veritas Support website:

[www.veritas.com/support](http://www.veritas.com/support)

## Device configuration status code 3

**Message:** Could not get host name

**Explanation:** An attempt to look up the host name for this host failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the host name is resolvable.

## Device configuration status code 7

**Message:** Invalid SCSI port number for the robot

**Explanation:** A request was made to add or change the SCSI port number for a robot, but the SCSI port number provided was not valid.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify the correct SCSI port number for the robot. Perform device discovery by using the **Device Configuration Wizard**, or check the Windows registry as needed to obtain the SCSI port number.

## Device configuration status code 8

**Message:** Invalid SCSI bus number for the robot

**Explanation:** A request was made to add or change the SCSI bus number for a robot, but the SCSI bus number provided was not valid.

**Recommended Action:** Specify the correct SCSI bus number for the robot. Perform device discovery by using the **Device Configuration Wizard**, or check the Windows registry as needed to obtain the SCSI bus number.

## Device configuration status code 9

**Message:** Invalid SCSI target for the robot

**Explanation:** A request was made to add or change the SCSI target for a robot, but the SCSI target provided was not valid.

**Recommended Action:** Specify the correct SCSI target for the robot. Perform device discovery by using the **Device Configuration Wizard**, or check the Windows registry as needed to obtain the SCSI target.

## Device configuration status code 10

**Message:** Invalid SCSI logical unit number for the robot

**Explanation:** A request was made to add or change the SCSI logical unit number for a robot, but the SCSI logical unit number was not valid.

**Recommended Action:** Specify the correct SCSI logical unit number for the robot. Perform device discovery by using the **Device Configuration Wizard**, or check the Windows registry as needed to obtain the SCSI logical unit number.

## Device configuration status code 11

**Message:** Invalid Usage

**Explanation:** Either one of the Media Manager device configuration commands (`tpconfig` or `tpautoconf`) was executed with improper options, or an incompatibility exists between the components or the versions of the product.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the `tpconfig` or the `tpautoconf` usage statement for the expected usage and compare with the parameters that are being sent to start the new process.
- Verify that all of the Media Manager binaries are at a compatible version level.

## Device configuration status code 13

**Message:** Failed reading drive or robot config file

**Explanation:** A request was made to list the device configuration, but an error was encountered while reading from the EMM database.

**Recommended Action:**

- Examine the daemon debug log and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that `nbemm` is running. Display the device configuration to determine whether or not the database is corrupt. Restore a saved copy of the databases from the catalog backups, or delete them and recreate the device configuration as needed.

## Device configuration status code 14

**Message:** Invalid drive index



**Explanation:** A request was made to add, update, or list a drive configuration entry, and the specified drive index was not associated with a configured drive.

**Recommended Action:**

- Display the device configuration to obtain the list of valid drives. Avoid making device configuration changes from multiple sources simultaneously.
- If more information is needed, examine the daemon debug log and the command or interface output for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 15

**Message:** Invalid robot number

**Explanation:** On a request to modify the device configuration, the specified robot number was not within the allowable range, the robot number did not correspond to a currently configured robot, or the robotic database is corrupted.

**Recommended Action:**

- Specify a robot number in the range from 0 to 32767.
- Ensure that all of the device configuration changes or deletions are performed on the devices that are currently part of the device configuration.
- Verify that `nbemm` is running. Restore a saved copy of the robotic database from catalog backups, or delete it and recreate any needed robotic configuration information.

## Device configuration status code 16

**Message:** A SCSI inquiry sent to the device has failed

**Explanation:** On a request to add or update a SCSI robotic library or drive, the Media Manager cannot obtain the device's serial number and inquiry string. The Media Manager obtains this information by sending a SCSI Inquiry command to the device. A failure indicates that NetBackup was not able to communicate with the device by using SCSI.

**Recommended Action:**

- Ensure that the device is physically connected.
- Ensure that the operating system is configured to recognize the device and that the operating system can see the device.
- Ensure that no other process uses the device and that the device is not offline.

## Device configuration status code 17

**Message:** This robot type does not support multiple media types

**Explanation:** An attempt to add or update a robotic drive failed because the drives in this robotic library are configured with a different drive type. (Some NetBackup robotic library types do not support multiple media types.)

See the [NetBackup Release Notes](#) or the [NetBackup Administrator's Guide, Volume II](#), for more information about the NetBackup robotic library types that support multimedia.

**Recommended Action:**

- Configure all of the drives for this robotic library with the same drive type.
- If you use the NetBackup Server and want a robotic library with multiple media types, contact Veritas to purchase the NetBackup Enterprise Server.

## Device configuration status code 18

**Message:** Invalid robot type

**Explanation:** On a request to modify the device configuration, the specified robot type was either invalid or it did not match the robot type for the robot that is associated with the specified robot number.

**Recommended Action:**

- Check the device configuration for configured robots, and specify the correct robot type applicable for the device configuration information being updated.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that all of the Media Manager binaries are at a compatible version level.

## Device configuration status code 19

**Message:** Invalid device path name

**Explanation:** On a request to change the device configuration, the specified device path or device name was not valid.

**Recommended Action:**

- To avoid configuring invalid device paths and device names, use the **Device Configuration Wizard** (on supported device discovery platforms). The wizard automatically configures device paths and device names.

- On Windows hosts, check the operating system configuration or registry for device names and refer to the `tpconfig` command in NetBackup online Help. Information for the UNIX and Linux hosts is available at the following location: See the [NetBackup Device Configuration Guide](#). Always use the no-rewind device files for the drives that are attached to UNIX and Linux hosts. Check to ensure that the specified device paths exist as character-special files. Check for detailed errors from the command or the user interface output.

## Device configuration status code 21

**Message:** Robot number is already in use

**Explanation:** On a request to add a robot to the device configuration, the robot number was found to be already in use for a different robot.

**Recommended Action:** Check the device configuration on all of the device hosts for configured robots, and specify a robot number that is not already in use. Use the following command to display all of the devices in the EMM database:

```
tpconfig -emm_dev_list
```

## Device configuration status code 22

**Message:** Device path is already in use

**Explanation:** On a request to add or change robot information in the device configuration, the specified robotic device path is already in use by another configured robot.

**Recommended Action:**

- To avoid configuring the device paths that are already in use, use the **Device Configuration Wizard** (on supported device discovery platforms). The wizard automatically configures the device paths and the device names.
- Display the device configuration by using the `tpconfig -d` command or a device configuration interface to see the robotic information that is already configured. Windows hosts have multiple ways to configure robots (that is, changer names or port, bus, target, or LUN). Check the operating system configuration or registry for changer names and their associated SCSI paths. Check for detailed errors from the command or the user interface output.

## Device configuration status code 24

**Message:** Incomplete robot information

**Explanation:** On a request to change the device configuration, some of the required robot information was not specified.

**Recommended Action:** Check the command usage and reissue the request with all of the required robot information specified.

## Device configuration status code 25

**Message:** Robot drive number in use for this robot

**Explanation:** On a request to change the device configuration, the specified drive address in the robot is in use by another drive in the device configuration.

**Recommended Action:** The drive address in the robot is the following: the robot drive number for most robot types, the ACS/LSM/PANEL/DRIVE coordinates for ACS robots, or a vendor drive name for TLH and TLM robots. Two drives cannot have the same drive address in a robot in a given device configuration. If the drive addresses need to be adjusted, delete one of the drives or make use of an unused drive address as a temporary state. For example, a robot has two drives with robot drive numbers 1 and 2 that need to be swapped. Change one drive to use robot drive number 3 temporarily. Then, change the other drive to use robot drive number 1 or 2 as appropriate. Finally, change the first drive to the open robot drive address 1 or 2.

## Device configuration status code 27

**Message:** Invalid drive type for the robot

**Explanation:** On a request to configure a drive to be in a robot, the drive type was not valid for the selected robot type.

**Recommended Action:** Check the Robot Attributes tables in the following manual to determine the valid media types for a given robot type:

See the [NetBackup Device Configuration Guide](#).

Drive types directly correspond to the listed media types. Configure the supported devices so that invalid combinations of drive types and robot types are not required.

## Device configuration status code 28

**Message:** Invalid robot drive number for the robot type

**Explanation:** On a request to configure a drive to be in a robot, the robot drive number was not valid for the selected robot type.

**Recommended Action:** The robot drive number (for ACS robots, the set of ACS drive identifiers) is limited to the ranges that are based on the robot type. These

limits are based on a supported device list. An invalid robot drive number means that the drive number was not within the acceptable range. Make sure that the robot hardware is supported and that the required patches are installed to support the robotic library. If the robot type is TLH or TLM, do not specify a robot drive number because the drives are addressed with a vendor drive name.

## Device configuration status code 29

**Message:** Drive index is in use by another drive

**Explanation:** On a request to add a drive to the device configuration, the requested drive index was in use on the targeted device host.

**Recommended Action:**

- To avoid configuring a drive index that is already in use, use the **Device Configuration Wizard** (on supported device discovery platforms). The wizard automatically configures the drive index.
- If you use a device configuration interface that allows the drive index to be specified, use the `tpconfig -d` command to determine the drive indexes that are already in use on the targeted device host. Then, specify a drive index that is not in use.

## Device configuration status code 30

**Message:** Robot number is in use by another robot

**Explanation:** On a request to add or update a robotic drive in the device configuration, the robot number and robot type specified were associated with an existing robot of a different robot type.

**Recommended Action:** Check the device configuration on the targeted device host and identify the configured robots. On the drive configuration request, specify both the robot number and the robot type that relate to the robot that contains the drive.

## Device configuration status code 31

**Message:** Robot number does not exist

**Explanation:** On a request to add or update a drive or robot in the device configuration, the robot number and the robot type specified were not associated with any configured robots on the targeted device host.

**Recommended Action:** Check the device configuration on the targeted device host and identify the configured robots. Every drive that is configured as a robotic drive must already have its robot configured on that device host. The shared robotic

libraries that have robotic control on a remote host must have a logical robotic entry that refers to the remote host having robotic control. Add the robot to the device configuration first. Then, add the drive. Define it to be in the robot. If the robot was already configured, specify the correct robot number and robot type on the drive or the robot configuration request.

## Device configuration status code 33

**Message:** Robot type must be controlled locally

**Explanation:** On a request to add or update a robot in the device configuration, a remote control host was specified for a library type that does not support it.

**Recommended Action:**

- Check that you configured the correct robot type.
- Configure the device with local control by using its local device path.

## Device configuration status code 34

**Message:** Drive name is already in use by another drive

**Explanation:** On a request to add or update a drive in the device configuration, the requested drive path was in use on the targeted device host.

**Recommended Action:**

- To avoid configuring any paths that are already in use, use the **Device Configuration Wizard** (on supported device discovery platforms). The wizard automatically configures the drive paths.
- Before you make configuration changes, either check the existing drive configuration through a device configuration interface, or use the `tpconfig -d` command to determine the drive paths that are already in use on the targeted device host. Then, specify a drive path that is not already in use.

## Device configuration status code 35

**Message:** Drive name does not exist

**Explanation:** On a request to update or delete a drive in the device configuration, there were no drives that had the specified drive name on the targeted device host.

**Recommended Action:** Check the device configuration on the targeted device host and identify the configured drives. When you make drive configuration changes or deletions, specify the drive name as it is configured. Ensure that you use the proper case.

## Device configuration status code 36

**Message:** <NONE>

**Explanation:** On a request to make a device configuration change, an error occurred. A detailed message appears in the command or the utility interface output.

**Recommended Action:**

- Examine the daemon debug log and command or interface output for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the device configuration request and examine the logs.

## Device configuration status code 37

**Message:** Residence is not licensed for shared drive support

**Explanation:** On a request to add or update a drive in the device configuration, the drive was specified as shared. No support for shared drives exists for that drive type or for the type of robot that is associated with the drive.

**Recommended Action:** Check the Veritas Technical Support website and product release documentation for supported device configurations. See the following URL for the Veritas Technical Support website:

[www.veritas.com/support](http://www.veritas.com/support)

## Device configuration status code 38

**Message:** Current version does not support remote device host

**Explanation:** On a request to change the EMM server, the specified host is not the local host. The current software is not licensed to allow remote hosts.

**Recommended Action:** Check the product documentation for the supported device configurations. Obtain an additional software license that allows remote hosts to be configured, or specify only local host names on the configuration request.

## Device configuration status code 39

**Message:** Adding this drive would exceed the maximum allowed

**Explanation:** On a request to add a drive to the device configuration, the licensed limit for the maximum number of drives was reached on the targeted host.

**Recommended Action:** Check the product documentation for the supported device configurations. Obtain an additional software license that allows more drives to be

configured, or limit the configuration to the number of drives that the current licensing allows.

## Device configuration status code 40

**Message:** Adding this device would exceed the maximum allowed

**Explanation:** On a request to add a robot to the device configuration, the licensed limit for the maximum number of robots was reached on the targeted host.

**Recommended Action:** Check the product documentation for the supported device configurations. Obtain an additional software license that allows more robots to be configured, or limit the configuration to the number of robots that the current licensing allows.

## Device configuration status code 41

**Message:** Cannot change terminal mode

**Explanation:** When an attempt was made to change the mode for terminal input between cooked and raw, a system call failed.

**Recommended Action:** Examine the user interface output for the system error that is associated with the failed system call. Then troubleshoot according to the operating system vendor recommendations.

## Device configuration status code 42

**Message:** Cannot create miscellaneous working repository

**Explanation:** On a device configuration request, the miscellaneous working directory or folder is not present and cannot be created.

**Recommended Action:** Find out why `/usr/openv/volmgr/misc` (UNIX and Linux) or `install_path\volmgr\misc` (Windows) cannot be created. On Windows, determine which accounts the NetBackup Volume Manager service and device configuration interfaces are running under. Compare them with the security properties of the database folder. On UNIX and Linux, determine if users or device configuration interface callers are running under a user and group with permissions to create the miscellaneous directory.

## Device configuration status code 44

**Message:** Cannot discover devices. See the [NetBackup Troubleshooting Guide](#) for details.



**Explanation:** Device discovery cannot obtain or verify its lock file or had a problem with the EMM server.

**Recommended Action:**

- Examine the daemon debug log and command or interface output for a more detailed message on the system error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation and examine the logs. One of the following may have occurred:
  - Lock file problems: The device discovery process sets a lockfile in the `/usr/opensv/volmgr/misc` (UNIX and Linux) or `install_path\Volmgr\misc` (Windows) directory named `tpac.lock`. It sets the lockfile to ensure that only one instance of discovery runs on a particular host. It then checks the lockfile before it updates the configuration.
  - Cannot obtain lockfile.  
The lockfile may be held by another discovery process. In this case, the following error is displayed:

```
another tpautoconf is already running
```

Use standard OS process tools (`ps` on UNIX and Linux or Task Manager on Windows) to determine if another `tpautoconf` process is running. If not, delete the lockfile and re-run device discovery. If another `tpautoconf` process is running, wait for it to complete before retrying.

- Failed the lockfile check.  
In the case of long device-discovery cycles, the interface may timeout or the user may cancel the process. Part of the timeout or cancelation is to remove the lockfile. This action tells the device discovery process that it should not continue making modifications to the device configuration. If action occurs, run the discovery process again.

## Device configuration status code 48

**Message:** RSM is not supported.

**Explanation:** On a request to make a device configuration change, the RSM (Microsoft Removable Storage Manager) robot type was specified, but it is no longer supported.

**Recommended Action:** Use a supported Media Manager robot type.

## Device configuration status code 49

**Message:** global device database host name is invalid.

**Explanation:** On a device configuration request, the EMM server name cannot be obtained.

The EMM server name is obtained through an internal request to read the bp.conf file (or Windows registry). This request is likely to fail if the EMMSERVER entry is not set.

**Recommended Action:** Use `tpautoconf -get_gdbhost` on a device host to obtain its EMM server name. Use `tpautoconf -set_gdbhost` to set the EMM server name, as needed.

## Device configuration status code 51

**Message:** No compatible device is registered at these SCSI coordinates.

**Explanation:** On a request to add or change robot or drive information in the device configuration, the specified SCSI coordinates did not correspond to a device in the system registry. This status code applies to Windows systems only.

**Recommended Action:** To avoid manually specifying the SCSI coordinates (port, bus, target, and LUN), use the **Device Configuration Wizard**. The wizard fully automates (on supported device discovery platforms) the device configuration requests. Use the **Media and Device Management** interface to browse for devices in the system registry. Check the operating system registry to ensure that devices are present at the specified coordinates when SCSI coordinates are manually configured.

## Device configuration status code 52

**Message:** The device name is not valid, no device responded.

**Explanation:** On a request to add or change robot or drive information in the device configuration, no device was found in the system registry with the specified device name. This error code applies to Windows systems only.

**Recommended Action:** To avoid manually specifying the device name, use the **Device Configuration Wizard**. The wizard fully automates (on supported device discovery platforms) device configuration requests. Use the **Media and Device Management** interface to browse for devices in the system registry. Check the operating system registry to ensure that the devices are present at the specified coordinates when the devices are manually configured.

## Device configuration status code 53

**Message:** Shared Storage Option (SSO) is not licensed

**Explanation:** An attempt to add a path to a drive failed. It failed because the SSO license was not installed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that an active SSO license is installed on all of the servers that have a path configured to this drive and the server where this operation is performed.

## Device configuration status code 55

**Message:** Invalid NDMP host name

**Explanation:** An invalid host name or no host name was specified.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use `tpconfig -dnh` to verify that the host has been configured.
- Check the usage of the `tpautoconf -list_snapvault_volumes` command.

## Device configuration status code 56

**Message:** Invalid NDMP user name

**Explanation:** An invalid user name or no user name was specified.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use the `tpconfig -dnh` command to verify that the host has been configured.

## Device configuration status code 57

**Message:** Internal NDMP error

**Explanation:** An error occurs on the NDMP device.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the usage of the `tpautoconf -probe` command.
- An error occurs while it tries to get the serial number and inquiry string for a device connected to an NDMP filer. Verify that the device is properly attached to the filer.

## Device configuration status code 58

**Message:** NDMP failed to verify host

**Explanation:** An error occurs while using the NDMP verify functionality.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the usage of the `tpautoconf -verify` command.
- Verify that the device is properly attached to the filer.

## Device configuration status code 59

**Message:** NDMP is not installed on platform

**Explanation:** The NDMP option is not installed on this server.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the NDMP option is properly installed and licensed.
- Verify that NDMP is supported on the platform in question.

## Device configuration status code 60

**Message:** Invalid NDMP password

**Explanation:** An invalid NDMP password or no password was provided.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the password is appropriate for the media server and filer pair.
- Verify that the password was provided correctly on the command or in the **NDMP Host** dialog box.

## Device configuration status code 61

**Message:** NDMP host exists, use change option

**Explanation:** An attempt to add a filer fails because the filer already exists in the EMM database.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use the `-update` option of `tpconfig` instead of the `-add` option.

## Device configuration status code 62

**Message:** NDMP host does not exist

**Explanation:** The NDMP host does not exist in the EMM database.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use the `-add -nh` option on the `tpconfig` command to add the NDMP host.

## Device configuration status code 63

**Message:** NDMP request failed

**Explanation:** An attempt to create an NDMP session failed, or an attempt to send an NDMP message failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify NAS filer licenses, supported operating system levels, and network connectivity.

## Device configuration status code 64

**Message:** Invalid NDMP device

**Explanation:** An invalid NDMP device was specified.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 65

**Message:** NDMP robot exists, use change option

**Explanation:** The robot currently exists in the EMM database.

**Recommended Action:** Use the **NetBackup Administration Console** or the `tpconfig -update -robot` command to change the robot configuration.

## Device configuration status code 66

**Message:** NDMP robot does not exist

**Explanation:** An update request was issued for a non-existent robot.

**Recommended Action:** Use the **NetBackup Administration Console** or the `tpconfig -update -robot` command to add the correct robot.

## Device configuration status code 67

**Message:** Unable to connect to NDMP host verify host name

**Explanation:** A network connection to the NAS host failed.

**Recommended Action:**

- Use the `tpautoconf -verify` command to verify the host name, user name, and password.
- Use the `ping` command to verify network access.

## Device configuration status code 68

**Message:** Unable to process NDMP message

**Explanation:** An unexpected error occurs while an NDMP message processed.

**Recommended Action:** Examine debug logs and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 69

**Message:** NDMP host not connected

**Explanation:** Unable to process the NDMP messages with the NDMP host.

**Recommended Action:** Examine the debug logs for more information on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 70

**Message:** Unable to create NDMP session

**Explanation:** An error occurs while opening an NDMP connection to a NAS filer.

**Recommended Action:**

- Examine debug logs for more information on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use the `tpautoconf -verify` command to verify the host name, user name, and password.
- Use the `ping` command to verify network access.

## Device configuration status code 71

**Message:** NDMP get\_host\_info failed

**Explanation:** The NAS host fails to correctly process the ndmp\_get\_host\_info protocol request.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 72

**Message:** NDMP get\_server\_info failed

**Explanation:** The NAS host fails to successfully process the get\_server\_info protocol request.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 73

**Message:** Unsupported NDMP version

**Explanation:** NetBackup supports tape devices on NDMP protocol versions V2, V3, and V4. For automatic device configuration, only V3 and V4 are supported.

**Recommended Action:**

- Examine debug logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- See your NAS vendor documentation for instructions on how to switch NDMP versions.

## Device configuration status code 74

**Message:** NDMP authorization error, verify username/password

**Explanation:** NetBackup fails to authenticate the user name or password on the NAS host.



**Recommended Action:** Use the `tpautoconf -verify` command to verify the user name and password.

## Device configuration status code 75

**Message:** NDMP config\_get\_mover\_type failed

**Explanation:** The NAS host fails to successfully process the config\_get\_mover\_type protocol request.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 76

**Message:** NDMP config\_get\_connection\_type failed

**Explanation:** The NAS host fails to successfully process the config\_get\_connection\_type protocol request.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device configuration status code 77

**Message:** Unable to connect to the EMM server

**Explanation:** A request was made to the EMM server, but it either did not reach the EMM server or resulted from a communication failure.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that `pbx_exchange` and `nbemm` are running.
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

## Device configuration status code 78

**Message:** The EMM server failed to process the request

**Explanation:** A request was made to the EMM server, but it either did not reach the EMM server or resulted from a communication failure.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that `pbx_exchange` and `nbemm` are running.
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

## Device configuration status code 79

**Message:** Unable to allocate memory for this process

**Explanation:** A memory allocation request failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that adequate memory is available.

## Device configuration status code 81

**Message:** This is a drive path operation, use the `-drpath` option

**Explanation:** A path operation was specified with the `tpconfig` command without the `-drpath` option. This error can occur when you try to change a drive's path using `tpconfig -update -drive`.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Check the `tpconfig` usage to ensure that the command is used properly and use `tpconfig -update -drpath` instead.

## Device configuration status code 82

**Message:** Add Drive Name Rule request failed

**Explanation:** A request to add a drive name rule failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- The rule being added already exists.
- The specified host does not exist in the EMM database. Use the `nbemmcmd -addhost` command to add the host to the EMM database.

## Device configuration status code 83

**Message:** Update Drive Name Rule request failed

**Explanation:** An update to a drive name rule failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- The rule being updated does not exist. Ensure that the drive name rule is entered correctly.
- The specified host does not have a local drive name rule configured. Configure a drive name rule.

## Device configuration status code 84

**Message:** Delete Drive Name Rule request failed

**Explanation:** A request to delete a drive name rule failed. You cannot add or delete a global drive name rule.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.
- A local drive name rule does not exist on the hosts specified.

## Device configuration status code 85

**Message:** List Drive Name Rule request failed

**Explanation:** Could not list the drive name rules for a given host or set of hosts.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the hosts are known in the EMM database.

## Device configuration status code 86

**Message:** Invalid Drive Name Rule

**Explanation:** A drive name rule was not specified, or contained an invalid character.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Observe the rules for drive names:
  - Cannot begin with a dash.
  - Cannot exceed 48 characters.
  - A literal field can only contain alphanumeric characters and plus (+), dash (-), period (.), or underscore (\_).
- An invalid field name was specified; check command usage.

## Device configuration status code 87

**Message:** System Error

**Explanation:** An operating system error occurred.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that adequate memory is available.
- Verify that Windows networking is properly installed.

## Device configuration status code 88

**Message:** Invalid host

**Explanation:** An attempt was made to add a device to a host that the EMM database does not recognize.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Use the `nbemmcmd -addhost` command to add the host to the EMM database.

## Device configuration status code 89

**Message:** Drive name rule has exceeded its maximum length of 48 characters

**Explanation:** The specified drive name rule is too long.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Choose a shorter rule.

## Device configuration status code 90

**Message:** Another device configuration is already in progress

**Explanation:** An instance of the **Device Configuration Wizard** or `tpautoconf` is already running.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation after the current instance is done.
- A lock on the device configuration cache may have been orphaned. Use the `nbemmcmd` command to clear the lock, then retry the operation.

## Device configuration status code 91

**Message:** The drive serial number already exists in the device database.

**Explanation:** An attempt was made to add a drive with a duplicate serial number.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the added drive has a unique serial number.

## Device configuration status code 92

**Message:** VxSS access denied

**Explanation:** A user attempts an operation without adequate permissions

**Recommended Action:**

- Verify that the user has the correct permissions to perform this operation.
- Verify that the authentication and authorization security settings are correct, under **Host Properties** in the **NetBackup Administration Console**.  
See the [NetBackup Security and Encryption Guide](#) for information on how to use the Veritas Product Authentication and Authorization Service.

## Device configuration status code 93

**Message:** Database server is down

**Explanation:** A request was made to the EMM Server, but the underlying database server does not respond.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- This error can occur if a cold catalog backup is in progress. Retry the request after this operation has completed.

## Device configuration status code 95

**Message:** The requested operation is not valid for the specified Disk Type

**Explanation:** The storage device you configured is not a disk storage device.

**Recommended Action:** Select an appropriate storage device.

## Device configuration status code 96

**Message:** The specified Disk Array Host is not configured in NetBackup

**Explanation:** You must first add this disk array host to the NetBackup host configuration before this operation can be performed. To view hosts, see the `nbemmcmd -listhosts` command in the [NetBackup Commands Reference Guide](#).

**Recommended Action:**

- If you try to update an existing host's credentials, this host no longer exists in NetBackup. It must be added again by using the `tpconfig` or the `nbemmcmd` command.
- The name you entered for the disk array host does not match any of the computer aliases in the NetBackup computer configuration. Use the `nbemmcmd` command to add the fully qualified array host name (or the name entered) to the computer alias list for your disk array.

## Device configuration status code 97

**Message:** No valid license key for Disk Array configuration

**Explanation:** Disk array snapshot support is a licensed featured. You must install the Snapshot Client license key before NetBackup can configure disk array credentials.

**Recommended Action:** Install the Snapshot Client license key.

## Device configuration status code 98

**Message:** OpenStorage feature is not licensed

**Explanation:** Credentials for OpenStorage servers cannot be added without the NetBackup OpenStorage license key.

**Recommended Action:** Install the license key with the OpenStorage feature enabled.

## Device configuration status code 99

**Message:** Credentials already exist

**Explanation:** Credentials already exist for the host that you are trying to add.

**Recommended Action:** Delete the existing credentials and then add the new ones.

## Device configuration status code 100

**Message:** NetBackup Snapshot Client not licensed

**Explanation:** Credentials for this type of host cannot be added without the NetBackup Snapshot Client license key. Host types that require this license are disk array manager servers and virtual machine servers.

**Recommended Action:** Install the NetBackup Snapshot Client license key.

## Device configuration status code 101

**Message:** authorization error, verify username/password

**Explanation:** The authorization failed with the given set of user name and password values.

**Recommended Action:** Verify the values that are provided and check for typographical errors.



# Device management status codes

This chapter includes the following topics:

- [Device management status codes](#)

## Device management status codes

These status codes appear in exit status and command output for the `ltid`, `tpclean`, `tpreq`, and `tpunmount` commands, and in system or debug logs. Programs that call those commands, such as media and device management user interfaces and the `vmopr cmd` command also presented these codes.

### Device management status code 1

**Message:** Invalid Drive Type/Density

**Explanation:** An invalid density was specified for the `-d` parameter on `tpreq`.

**Recommended Action:** Check the `tpreq` man page (command description) for the list of valid densities. Submit the mount request again with a valid density.

### Device management status code 2

**Message:** Drive is currently assigned

**Explanation:** A request was made for a specified drive, but the drive was assigned.

**Recommended Action:** Display drive status (by using the `vmopr cmd -d` command or other means) to see the list of drives and their assignment status. Run the request later or first clear the drive assignment: stop application activity on the drive, unmount the media with `tpunmount`, or reset the drive. If the wrong drive was specified,

submit the request again. Specify the correct drive name or index as appropriate for the interface being used.

## Device management status code 3

**Message:** Error in Sending Operator Message

**Explanation:** An attempt was made to send an operational message to `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

## Device management status code 4

**Message:** Error in Receiving Operator Message

**Explanation:** An attempt was made to receive a message from `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Investigate whether `ltid` is tied up in communications with devices or other components.

## Device management status code 5

**Message:** Error in Sending Daemon Message

**Explanation:** `ltid` made an attempt to send an internal process communications message to a robotic daemon or process by using an already existing internal message queue. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Investigate whether the robotic daemon or process on the local device host is tied up in communications with devices or other components.

## Device management status code 6

**Message:** Error in Receiving Daemon Message

**Explanation:** `ltid` attempted to receive or process an internal process communications message to a robotic process by using an existing internal message queue. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues, or mismatched software components.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

## Device management status code 7

**Message:** Error in Sending User Message

**Explanation:** `ltid` made an attempt to send a user message to `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

## Device management status code 8

**Message:** Error in Receiving User Message

**Explanation:** An attempt was made to receive a user message from `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues. On Windows, this error can also occur if an internal-system-registered event cannot be opened.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

## Device management status code 10

**Message:** IPC sequence error

**Explanation:** An internal process communications message sequencing error has occurred.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device management status code 12

**Message:** Invalid Operator

**Explanation:** An internal list of operators cannot be obtained.

**Recommended Action:** This error is an unexpected internal error. Stop and restart `ltid` (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

## Device management status code 13

**Message:** Error in IPC SHMGET call

**Explanation:** A process was unable to get a shared memory identifier associated with a segment of shared memory that `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

## Device management status code 14

**Message:** Error in IPC SHMAT call

**Explanation:** A process was unable to attach a shared memory segment that `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see what resources are currently in use.

## Device management status code 15

**Message:** The drive is DOWN

**Explanation:** An attempt was made to mount media on a drive or to reserve a shared drive that was logically configured to the DOWN state.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the application log files (such as the `bptm` log) to see why the drive may have been configured DOWN.
- Check the integrity of the drive, drive path, and media.

## Device management status code 16

**Message:** No mount pending for given mount index

**Explanation:** An attempt was made to retrieve information about a pending mount request, but no such pending mount request was found.

**Recommended Action:** Use a device monitor interface or consult application logs to see whether the request was completed or canceled. Requests to retrieve information for pending mount requests are valid only when the mount request is ongoing.

## Device management status code 17

**Message:** Drive does not support pending request density

**Explanation:** A drive was selected that has a drive type which is not compatible with the requested density.

**Recommended Action:**

- Allow the drive selection to be determined automatically.
- When you select the drive manually, check the device configuration and the valid density table (available in the `tpreq` man page or command description). Then, specify a drive that is compatible with the requested density.

## Device management status code 19

**Message:** Only the administrative user can perform the requested operation

**Explanation:** Either an attempt was made to stop `ltid` (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows). Or the `tpclean` command was called, but the user was not root (UNIX and Linux) or the administrator (Windows).

**Recommended Action:** If appropriate, give the user or the process administrator privileges on Windows or root privileges on UNIX and Linux and retry the operation.

## Device management status code 20

**Message:** Cannot stop device daemon with tapes assigned

**Explanation:** An attempt was made to stop `ltid`, but the media is currently mounted and assigned. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:** Halt all jobs that reference media, unmount all media, and stop all applications from using Media Manager before trying to stop `ltid`. If you can't unmount the media through the application interface, check for the existence and permissions of the `.ltisymlinks` file in the `/usr/openv/volmgr/misc` directory or in the `install_path\Volmgr\misc` folder. Initiate `tpunmount filename` for each line in the `.ltisymlinks` file, where *filename* specifies the contents of a line in that file. For example, on UNIX and Linux, the command may look like the following:

```
tpunmount /usr/openv/netbackup/db/media/tpreq/A00001
```

## Device management status code 21

**Message:** The drive is not ready or inoperable

**Explanation:** A drive was selected for a mount request, but the drive is not ready with loaded media.

**Recommended Action:** Wait until the drive is ready before you manually assign a drive to a pending mount request.

## Device management status code 22

**Message:** IPC Error: Daemon may not be running

**Explanation:** A request to `ltid` cannot be serviced. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on

Windows.) `ltid` is probably not running. If `ltid` is still running, its process lock file may have been removed. Also, message queues may not function correctly on the system.

**Recommended Action:**

- If `ltid` is not running, start `ltid` and try the operation again. On UNIX and Linux, run `/usr/openv/volmgr/bin/ltid`, and on Windows, start the NetBackup Device Manager service.
- If `ltid` is already running, check for the existence and permissions of the lock file itself and the lock file directory, that are as follows:  
`/usr/openv/volmgr/misc/.ltipid` (UNIX and Linux) or `install_path\Volmgr\misc\ltipid` (Windows). Terminate the `ltid` process if it is running. Create the lock directory or folder and adjust the permissions as needed so that `ltid` can obtain the lock.
- On UNIX and Linux, check the `msgget` man page and look for suggestions on how to troubleshoot the system message queues.

## Device management status code 23

**Message:** Invalid Drive Number

**Explanation:** A request was made for drive, but no such drive can be found in the active configuration.

**Recommended Action:** Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) Display the device configuration (by using `tpconfig -d` or other means) to view the list of valid drives. Specify the drive name or index as appropriate for the interface being used.

## Device management status code 24

**Message:** Requested drive cannot be reserved

**Explanation:** An attempt was made to reserve a shared drive, but the drive reservation request failed. This status code is related to the internal implementation of the SSO feature. It is not related to SCSI Reserve or Release.

**Recommended Action:** This condition is expected for any shared drives that are retried automatically. If problems persist, verify that the EMM server services requests and it does not list drives as reserved to hosts that currently do not use the drives.



## Device management status code 25

**Message:** File name does not exist

**Explanation:** A logical tape file or help file cannot be found. The `tpunmount` command was probably issued with a logical tape file specified that does not exist for this user.

**Recommended Action:** Check for existence of the logical tape file at the file path specified. The specified file path must match the exact case-sensitive path that was used when the tape mount was requested. Submit the request again with the correct file path. If the condition occurs during operator display of a pending request error message, check to see if the help files are properly installed at the following:

`/usr/openv/volmgr/help/robots/robot_type/help_file_name` (UNIX and Linux)  
or at `install_path\Volmgr\Help\Robots\robot_type\help_file_name` (Windows).

## Device management status code 26

**Message:** Request terminated because the host was not validated for volume pool

**Explanation:** The host where the mount request was initiated is denied access to the media. It is denied due to defined permissions for the volume pool in which the media ID is contained.

**Recommended Action:**

- Query the volume pool information for the requested volume pool on the host where the mount request was issued by running `vmpool -listall -b`. Check the system log to obtain the name of the host where the mount request originated. This host name is the one returned by the system `hostname(1)` command.
- Change the volume pool host name security with `vmpool` or another user interface that supports volume pool host attributes. Or change the volume pool that is associated with the volume (if it is not assigned). Or log on to the host that can use media in the targeted volume pool. Then, submit the mount request again.

## Device management status code 27

**Message:** Request terminated because media ID is expired

**Explanation:** A mount request was canceled because the media was requested with write access, and the media has expired.

**Recommended Action:** Request read-only access to the media on the mount request if a read-only operation is needed. Replace the media or change the expiration date to a future date that is based on the site policy. Use the media

management interface to view and change the expiration date for the media. Check and correct the system date and time, as needed.

## Device management status code 28

**Message:** Error in MsgGet

**Explanation:** `ltid` made an attempt to obtain a message queue identifier that was used for internal message communications. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) The request failed due to a system error. The error probably indicates a lack of system resources for message queues, or mismatched software components.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

## Device management status code 30

**Message:** Request terminated because media ID will exceed maximum mount count

**Explanation:** A mount request has been canceled because the media being requested has reached the maximum mount count that is associated with the media.

**Recommended Action:** Replace the media or change the maximum mount count to a higher value that is based on the site policy. A media management interface can be used to view and change the maximum mounts allowed for the media. Check that the number of mounts for the media is set to a reasonable value given the media's usage history. Correct it as needed by using `vmchange`.

## Device management status code 32

**Message:** Error in getting semaphore

**Explanation:** `ltid` made an attempt to obtain a semaphore that was used for arbitrating access to shared memory. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) The

request failed due to a system error. The error probably indicates a lack of system resources for semaphores, or mismatched software components.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

## Device management status code 33

**Message:** Error in SEMAPHORE operation

**Explanation:** A process was unable to perform a semaphore operation (such as lock or unlock) associated with resources maintained by `ltid`. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see what resources are currently in use.

## Device management status code 35

**Message:** Request terminated because media is unavailable (in DOWN drive, misplaced, write protected or unmountable)

**Explanation:** A mount request was canceled because the media being requested is not available. It may be in a DOWN drive or misplaced, write protected, or unmountable. Another possible cause of this message is that you are using a cleaning tape with no cleanings remaining.

**Recommended Action:** Use robotic inventory or manual means to compare the contents of media in the robotic library with the volume configuration. Then, update the configuration as needed. Determine the physical location of the media. Check integrity of the drive, drive path, and media if the media is found in a logically DOWN drive. Verify that the media is not a misconfigured cleaning tape. Move the media

into the robotic library and update the volume configuration if the media was not present in the library. Set the cartridge tab to allow write access, or request the media with read-only access if the write protection was the cause of the error.

If the problem is a cleaning tape with no cleanings remaining, replace the cleaning tape.

## Device management status code 36

**Message:** Request terminated by tpmount call from another process

**Explanation:** A request was made to change the limit for the following: the number of times that a volume can be mounted with write access for one or more volumes in the volume configuration. The value specified was not within the acceptable range. The maximum number of mounts value may also be invalid in the number of mounts and cleanings field of a barcode rule.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Specify a maximum-mounts value within the range of 0 to 2,147,483,647.

## Device management status code 37

**Message:** Drive being assigned is either not NDMP or on the wrong NDMP client

**Explanation:** A mount request was canceled because the request was targeted to a drive configured as attached to an NDMP client. The request was manually assigned to a drive other than the requested drive. The assigned drive is either not NDMP or it is an NDMP drive configured to a different client.

**Recommended Action:** Display the device configuration to determine which drives are configured as being attached to specific NDMP clients. Ensure that `ltid` was stopped and restarted after the last configuration changes were made. Reissue the request and assign it to a drive that is attached to the requested NDMP client.

## Device management status code 38

**Message:** Character device name for drive is not a character device

**Explanation:** On a tape mount request, the configured tape drive's no-rewind-on-close device file was neither a character-special device nor of a known type such as NDMP. (NDMP does not need to be a character special file.)

**Recommended Action:**

- To avoid configuring invalid device paths and device names, use the **Device Configuration Wizard** (on supported device discovery platforms). The wizard automatically configures paths and device names for tape drives.
- Always use no-rewind tape device files or recognized drive name syntax (such as for NDMP) for tape drives. Make sure that the specified device paths exist as character-special files. Check for detailed errors from the command or the user interface output.

See the [NetBackup Device Configuration Guide](#).

## Device management status code 39

**Message:** Parameter is invalid

**Explanation:** The `tpclean` command was called with invalid arguments, or an internal function encountered a missing reference to data it requires.

**Recommended Action:**

- If a cleaning operation was requested, check the `tpclean` usage statement and compare with the parameters that were specified.
- Check the installed software components and verify that they are all at a compatible release version.

## Device management status code 40

**Message:** File name already exists

**Explanation:** On a tape mount request, the file name that is associated with the request already exists or is already associated with another mount request.

**Recommended Action:** Submit the request again with a different file name. Specify a file name that does not correspond to an existing file. Or specify a file name that is not in use for another mount request that may be in progress.

## Device management status code 41

**Message:** Unknown drive name

**Explanation:** A request was made for a specified drive, but no such drive can be found in the active configuration. This status can occur in the following situations: if the device files are corrupt or missing, if they cannot be opened or read, or if there are no devices configured.

**Recommended Action:**

- Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) Display the device configuration (use the `tpconfig -d` command or other means) to see the list of valid drives. Specify the drive name or index as appropriate for the interface being used.
- Check integrity of the EMM database. Display the device configuration to do the following:
  - Determine if the database is corrupt.
  - Restore a saved copy of the database file from catalog backups, or remove the devices and recreate the device configuration.

## Device management status code 42

**Message:** Incorrect `tpreq` access mode

**Explanation:** On a tape mount request, the specified access mode was invalid. On a Windows hosts, a user without Administrator privileges made a request for the NetBackup Device Manager services.

**Recommended Action:** When you use `tpreq`, specify an access mode argument of `r` for read, `w` for write, or use the default (read) access mode. When you make any requests that require the NetBackup Device Manager services on Windows, do so under an account with Administrator privileges.

## Device management status code 44

**Message:** You do not have permission to create the file

**Explanation:** On a tape mount request, the file name that is associated with the request cannot be created due to directory permissions or folder permissions.

**Recommended Action:** Check for the existence of a file at the file path specified. If a file is found, delete the file if it is not needed or submit the request again and use a different file path. If no file exists at that location, check the directory permissions or the folder permissions for the following: read and write access for the user or the application process that issued the mount request.

## Device management status code 46

**Message:** Tape needs to be write enabled

**Explanation:** On a tape mount request, the specified access mode was for write access, but the physical media was write-protected.

**Recommended Action:** Change the physical media write-protect setting to allow write access (unlocked), or submit the request again with read-only access. To request read-only access by using `tpreq`, specify an access mode argument of `r` for read or use the default (read) access mode.

## Device management status code 47

**Message:** Unable to establish scan host for shared drive

**Explanation:** On a request to change a shared drive's status, an attempt to establish a connection to the drive's scan host failed.

**Recommended Action:**

- Determine which host serves as the drive's scan host: use the `vmopr cmd` output or check the Device Monitor in the **NetBackup Administration Console**.
- Ensure that `vm`d (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) is running on the scan host. On the scan host, examine debug logs and system logs for any messages that are related to the error.
- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- The detailed reason for the canceled request should be available in the daemon debug logs on the scan host. Correct the problem and submit the request again if needed.

## Device management status code 48

**Message:** Host is not the scan host for this shared drive

**Explanation:** On a request to assign, reserve, or scan a drive, the targeted device host determined that it was not the scan host for the drive. The request was refused (the caller retries it).

**Recommended Action:**

- If problems are encountered as a result of the reported error, check for communication, configuration, and system problems among the associated hosts. To check, use the `vmopr cmd` output or check the **NetBackup Administration Console Device Monitor**.

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Configure the scan ability priorities for assigning scan hosts by changing the Media Manager configuration. Configure it so that fewer network connections need to be maintained, and a greater system load is placed on hosts with more capability to service the load.

## Device management status code 49

**Message:** Tape file path exceeds 255 character maximum

**Explanation:** On a tape mount request, the file name that is associated with the request exceeds 255 characters.

**Recommended Action:** When you request a tape mount, ensure that the file name does not exceed 255 ASCII characters in length. If the mount requests come from an application, request an application change to use a shorter file name. Or install the product in a directory or a folder that does not cause the file name limit to be exceeded.

## Device management status code 50

**Message:** No action pending for given mount index

**Explanation:** On a request to obtain the pending action for a mount request, no known pending action was associated with the request.

**Recommended Action:** Use a device monitor interface to display any requests that have pending actions. Perform requests (like assign, deny, display, or resubmit) only on the requests that have pending actions.

## Device management status code 52

**Message:** No robot is defined of this type

**Explanation:** On internal communications between a robotic daemon or process and `ltid`, no robots of the expected type were found actively configured. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:** Display the running robotic processes to see if processes from a previous configuration are still running. If any are found, terminate them. Check the installed software components and verify that they are all at a compatible release version.



## Device management status code 53

**Message:** Request has been queued (Cancel to clear message)

**Explanation:** A mount request or drive-related operation was queued because drive resources were in use.

**Recommended Action:** Wait until the drive resources become available, or cancel pending mount requests as needed.

## Device management status code 55

**Message:** Operator denied mount request

**Explanation:** The operator denied a mount request.

**Recommended Action:** This error occurs when an administrator or operator cancels a user or an application mount request. The request may have been canceled for a number of reasons: missing or faulty media, or the need to allow other, higher priority requests to obtain drive resources. Check with the administrator or operator for more information.

## Device management status code 56

**Message:** Mount canceled, device daemon is terminating

**Explanation:** Pending mount requests were canceled because the administrator terminated `ltid` (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

**Recommended Action:** Wait for `ltid` to be restarted before you submit the request again. Check with the administrator as needed to determine daemon or service availability.

## Device management status code 58

**Message:** The device is not robotic, cannot perform cleaning

**Explanation:** An attempt was made to automatically clean a drive, but the drive is not in a robotic library.

**Recommended Action:** Clean standalone drives by inserting a cleaning tape when needed. For non-shared drives, update the cleaning statistics with `tpclean` or another user interface that supports cleaning-related operations.

## Device management status code 59

**Message:** No cleaning tape is defined in the device's robot or 0 cleanings remain.

**Explanation:** Either an attempt was made to automatically clean a drive, but no usable cleaning media is available, or the number of cleanings that remains for the cleaning tape is zero.

**Recommended Action:**

- Ensure that cleaning media was added to the robotic library for each drive type capable of being cleaned with a separate cleaning cartridge.
- Ensure that a positive number of cleanings is available for the cleaning media in the EMM database for the robotic library. Replace the cleaning tape or increase the number of cleanings for the cleaning media before the count reaches zero.
- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device management status code 60

**Message:** Robot daemon and/or robotic hardware is not available

**Explanation:** A robot was not configured or was operationally unavailable. Specifically, an attempt may have been made to automatically clean a robotic drive, but the robot is not defined or is unavailable. Alternatively, on an attempt to initialize the shared drive lists, a drive was found to be configured as robotic, without the required robot configured.

**Recommended Action:** Display the device configuration and ensure that the drive and robotic configuration information are consistent. Check the operational status of the robot and robotic software by checking the system log files. If more detail on robot operational status is needed, increase the level of verbosity by adding the `VERBOSE` option in the `vm.conf` file. Then, restart `ltid` (the device daemon /NetBackup Device Manager service).

## Device management status code 61

**Message:** No media found in device or robot slot, please verify

**Explanation:** On a request to mount media, no media was found in the targeted location before a designated time period had elapsed.

**Recommended Action:** Resubmit the request, and mount the media in the targeted drive before the designated time period has elapsed. Check the device configuration to ensure that the correct drive name has been configured and that `ltid`, the device daemon, was restarted after the last device configuration change was made.

## Device management status code 62

**Message:** Drive not available in library for mount request

**Explanation:** A mount request has been canceled because no drive is available. All compatible drives may be DOWN, or oversubscribed due to other active mount requests.

**Recommended Action:** Investigate device availability and scheduling/drive utilization of applications requesting drive resources. Under some conditions, mount requests are canceled so that they can be reissued at a later time when compatible drive resources are available.

## Device management status code 63

**Message:** Request terminated because mount requests are disabled

**Explanation:** A mount request was canceled because it cannot be satisfied.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

The detailed reason for the canceled request should be available in the system log, command output, or from a device monitor interface. Correct the problem and resubmit the request if needed.

## Device management status code 64

**Message:** Cannot assign a robotically controlled device

**Explanation:** An attempt was made to manually assign a specific device to satisfy a mount request, and the chosen device was configured in a robotic library.

**Recommended Action:** Assign the request to a standalone drive, or allow requests for mounts in robotic drives to be automatically assigned.

## Device management status code 65

**Message:** Invalid volume pool specified

**Explanation:** On a mount request, the media pool specified was not valid.

**Recommended Action:** Resubmit the request, specifying a volume pool name that is no more than 20 ASCII characters in length.

## Device management status code 66

**Message:** Request terminated because of volume pool mismatch

**Explanation:** The volume pool that is specified on the `tpreq` command did not match the volume pool in the Media Manager configuration for the media ID.

**Recommended Action:** Use a media management interface to obtain the volume pool name of the media that is to be mounted. Then resubmit the mount request, specifying the correct pool name.

## Device management status code 69

**Message:** Request terminated because media is unmountable

**Explanation:** A mount request has been canceled because the media being requested is not mountable. The same media has been found to be unmountable in at least two different drives.

**Recommended Action:**

- Check integrity of the drive, drive path, and media.
- Verify that the media is not a misconfigured cleaning tape.

## Device management status code 70

**Message:** Request terminated because media is write protected

**Explanation:** A mount request has been canceled because the media being requested for write access is not write-enabled.

**Recommended Action:** Check the physical media cartridge to see whether write-protection has been enabled. If write access to the media is desired, disable write protection for the media.

If read-only access is desired, leave the write-protection enabled. Then make the necessary administrative requests in the requesting application (such as suspending the media) to ensure that the media is requested only for read access.

If the media was requested through the command line interface, see the `tpreq` man page or command description for specifying the media access mode. The `tpreq` command is described in the following manuals:

See the [NetBackup Administrator's Guide, Volume II](#).

See the [NetBackup Commands Reference Guide](#).

## Device management status code 71

**Message:** Request terminated because media is a cleaning tape

**Explanation:** A mount request has been canceled because the media that was found in the drive is a cleaning tape.

**Recommended Action:** Check to make sure that the Media Manager's EMM database is up-to-date. If there are cleaning media in the library, assign appropriate cleaning media types to them in the Media Manager EMM database.

## Device management status code 72

**Message:** EMM library call failed

**Explanation:** A request that was made to read/write data to EMM failed.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that pbx\_exchange is running.
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and accepting new connections.

## Device management status code 73

**Message:** Stopping device daemon with tapes assigned

**Explanation:** An operator requested that `ltid` shutdown but tapes are still in use.

**Recommended Action:** None. This message is advisory and no action is required.

## Device management status code 74

**Message:** Robot operation failed

**Explanation:** A tape mount by `bptm` resulted in a failed robotic operation.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the robotic hardware is functional.

## Device management status code 75

**Message:** LTI system error

**Explanation:** A system error occurred.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- A `tpclean` operation was attempted and Windows networking was not properly configured.
- A `malloc` system call failed when trying to stop `ltid`.

## Device management status code 76

**Message:** Robot/LTI protocol error

**Explanation:** Communication between `ltid` and the robotic daemons caused a protocol error.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that `ltid`, `bptm`, and the robotic daemons are at a compatible NetBackup level.

## Device management status code 77

**Message:** VxSS access denied

**Explanation:** A user tried to run `tpclean` without adequate permissions.

**Recommended Action:**

- Verify that the user is logged on with permissions adequate for this operation.
- Verify that the VxSS settings are correct, under **Host Properties** in the **NetBackup Administration Console**.  
See the [NetBackup Security and Encryption Guide](#).

## Device management status code 78

**Message:** Unable to connect to the EMM server

**Explanation:** An attempt to retrieve or update information in EMM failed.

**Recommended Action:**

- Verify that the correct EMM server name is listed in the NetBackup configuration.
- Verify that the media server that encounters this error is listed in the NetBackup configuration on the EMM server.
- Verify that EMM is running on the EMM server.
- Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Device management status code 79

**Message:** Cannot retrieve Job ID from Job Manager

**Explanation:** The `tpreq`, `tpclean`, or `tpunmount` command encountered an error while it tries to get a job ID from the NetBackup Job Manager.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that the NetBackup Job Manager is running on the master server.

## Device management status code 80

**Message:** Job Manager returned error: see activity monitor

**Explanation:** The `tpunmount` command encountered an error while communicating with the NetBackup Job Manager. The details of this issue may be found in the Activity Monitor entry for this job.

**Recommended Action:**

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Verify that the NetBackup Job Manager is running on the master server.
- Verify that the arguments that are provided to the `tpunmount` command are correct.

## Device management status code 81

**Message:** Retry later

**Explanation:** An attempt was made to use resources that are controlled by EMM. These resources were not available.

**Recommended Action:** Retry the command at a later time.

## Device management status code 82

**Message:** No drive available

**Explanation:** An attempt to use a drive was made but that drive was not available.

**Recommended Action:**

- Verify that the drive is not DOWN on the intended media server.
- Verify that the media server where the drive is found is ACTIVE.
- Retry the command with a different drive.

## Device management status code 83

**Message:** Media does not exist in database

**Explanation:** The requested media ID was not found in the EMM database.

**Recommended Action:**

- Verify that the requested media ID was entered correctly.
- Retry with a different media ID.

## Device management status code 84

**Message:** No Error on operation, sideband data only

**Explanation:** This is only an informational message.

**Recommended Action:** No action is required by the user.



# Robotic status codes

This chapter includes the following topics:

- [Robotic status codes](#)

## Robotic status codes

Robotic daemons or processes issue these status codes. They are also issued by the programs that call the robotic operations, such as the `vmchange` command and the media and device management user interfaces.

### Robotic status code 200

**Message:** STATUS\_SUCCESS

**Explanation:** A robotic operation was successfully completed.

**Recommended Action:** None

### Robotic status code 201

**Message:** Unable to open robotic path

**Explanation:**

The robotic library device cannot be opened due to one of the following reasons:

- The robot device, path, or library name in the device configuration may not be valid.
- The configured robotic device may not exist.
- The robotic device may be incorrect, such as a UNIX and Linux device file that does not have a character special file format.
- The robotic daemon/process lock file cannot be opened or a lock obtained.

- The open operation on the device or through the API interface (such as NDMP) failed.

**Recommended Action:**

- Stop any robot test utilities that may be running, since they have the lock on the robotic device when they are active.
- Check the configuration of the robot against the recommended configuration as indicated in the robot configuration documentation.
- Check the health of the robotic device by using a robot test utility, then close the test utility when finished.
- Check for the existence and permissions of the lock file itself and the lock file directory, which is `/usr/opensv/volmgr/misc/vmd.lock` (UNIX and Linux) or `install_path\Volmgr\misc\vmd.lock` (Windows). Create the directory/folder and adjust the permissions as needed so that the robotic daemon/process can use the lock file. Stop and restart `ltid` (the device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

## Robotic status code 202

**Message:** Unable to sense robotic device

**Explanation:**

An element of the robotic library device cannot be sensed. The cause can be any of the following:

- The SCSI commands mode sense, mode select, or read element status (of slot, drive, transport, i/e element) may have failed.
- A network API-controlled library inventory request may have failed.
- The robotic daemon/process cannot initialize a robotic database file.

**Recommended Action:**

- Check the configuration of the robot against the recommended configuration as indicated in the robot configuration documentation.
- Check the health of the robotic device by using a robot test utility and then close the test utility when finished.
- Check for the existence and permissions of the temporary robotic database and the temporary database directory/folder, which is `/usr/opensv/volmgr/misc/robotic_db` (UNIX and Linux) or `install_path\Volmgr\misc\robotic_db` (Windows). Create the directory/folder and adjust the permissions as needed so that the robotic daemon/process can

create it or use it. Stop and restart `ltid` (the device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

## Robotic status code 203

**Message:** Timeout waiting for robotic command

**Explanation:** A robotic operation timed out because it did not return with a status before the designated time period elapsed.

**Recommended Action:**

- Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.
- Check whether excessive hardware retries have delayed the completion of a robotic command.
- Check to see whether the robotic device still functions. Use a robot test utility to send commands to the device to see whether it is responsive. Execute `vmps` to verify that no unexpected Media Manager processes are running. Some processes should remain running, but some processes that do not go away can indicate a more serious problem, such as a hung system call.

## Robotic status code 204

**Message:** Unable to initialize robot

**Explanation:** The robot cannot be initialized. This generic status is used for many conditions.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the system log messages that are related to the specific error leading to the robot initialization failure.

## Robotic status code 205

**Message:** Robotic mount failure

**Explanation:** The robot cannot mount media.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the system log messages that are related to the specific error leading to the media mount failure.

## Robotic status code 206

**Message:** Robotic dismount failure

**Explanation:** The robot cannot dismount media.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the system log messages that are related to the specific error leading to the media dismount failure.

## Robotic status code 207

**Message:** Invalid command code

**Explanation:** A robotic operation was requested with improper options, when it was not supported, or a robotic operation encountered an incompatible device interface. There may be an incompatibility between components or versions of the product.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that all of the Media Manager binaries and user interfaces are at a compatible version level.

## Robotic status code 208

**Message:** Requested slot is empty

**Explanation:** No media was found in a specified slot. The volume configuration may not be consistent with the physical contents of the robotic library that is associated with the volume.

**Recommended Action:** Install or realign the container/holder for the media if it is misplaced or misaligned. Place media right-side-up in the slot if the media is upside-down. Check to see if the requested slot is reserved to the robotic library for internal use. Physically correct issues within the robotic library, or use a media management interface to correct the volume configuration.

## Robotic status code 209

**Message:** Unable to open drive

**Explanation:** The drive cannot be opened. The drive configuration may be incorrect and the drive may be logically DOWN. Also, the drive may never have become ready after media was placed in the drive.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check for improperly configured cleaning media or interference with the drive cleaning operation. Check for bad media that may have led to the drive not becoming ready after media was placed within it.
- To avoid configuring incorrect device paths and device names, which is a common cause of drive open problems, use the **Device Configuration Wizard** (on supported device discovery platforms) so that device paths and device names can be automatically configured. Investigate the system log messages that are related to the specific error leading to the open failure.

## Robotic status code 210

**Message:** Unable to SCSI unload drive

**Explanation:** The drive cannot be unloaded. The drive configuration may be incorrect and the drive may be logically DOWN. Also, the drive may never have become ready after media was placed in the drive.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Check for improperly configured cleaning media or interference with the drive cleaning operation. Check for bad media that can prevent unloading the drive. To avoid configuring incorrect device paths and device names, which is a common cause of drive unload problems, use the **Device Configuration Wizard** (on supported device discovery platforms) so that device paths and device names can be automatically configured. Investigate the system log messages that are related to the specific error leading to the unload failure.

## Robotic status code 211

**Message:** Process killed by signal

**Explanation:** An unexpected signal or event canceled the robotic operation.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check vendor or operating system administrative interfaces and logs to see if robotic commands are being canceled.

## Robotic status code 212

**Message:** Process killed by parent

**Explanation:** A robotic operation was canceled because of one of the following:

- It did not return a status before the designated time period elapsed
- Communications or hardware errors led to the need to reinitialize the device

**Recommended Action:**

- Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.
- Check to see if the robotic device still functions.
- Check if excessive hardware or communication problems have delayed the completion of a robotic command.
- Use a robot test utility to send commands to the device to see whether it is responsive. Execute `vmps` to verify that no unexpected Media Manager processes

are running. Some processes should remain running, but some processes that do not go away can indicate a problem, such as a hung system call.

## Robotic status code 213

**Message:** Drive does not exist in robot

**Explanation:** A targeted drive was not found in the robotic library. The drive configuration may be incorrect.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Obtain the list of drives using a method that involves a robotic library query, such as a query available from the robot test utility. Compare the list of drives against the device configuration. Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. `ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.

## Robotic status code 214

**Message:** Robot number does not exist

**Explanation:** A targeted robotic library was not found in the active device configuration.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) On commands to robotic libraries, specify only robotic libraries that are actively part of the device configuration.

## Robotic status code 215

**Message:** Requested tape in other or non-configured drive

**Explanation:** The targeted media was found in a drive differing from the targeted drive.

Requested media can be temporarily unavailable, which is normal. Also, media can remain unavailable until administrator or operator action is taken.

**Recommended Action:**

- If the media is needed immediately, examine the command output (if available), debug logs, and system logs for messages relating to the targeted media. See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check for conflicts between multiple applications using media in the robotic library. Check integrity of the drive and drive paths, so that media is not routinely left in other drives.

## Robotic status code 216

**Message:** Door is open on cabinet

**Explanation:** The robotic library door was open.

**Recommended Action:** Close the door of the robotic library and reissue the robotic request. See if the door latch mechanism works by comparing what happens with robot test utility commands when the door is open versus closed.

## Robotic status code 217

**Message:** Requested slot already has cartridge

**Explanation:** The requested slot was already held or was associated with a cartridge.

**Recommended Action:** Ensure that the inject/eject request does not target a slot that already contains media. Check for media in drives to ensure that the media's home slot location is not targeted for use with media to be injected.

## Robotic status code 218

**Message:** Cannot move from media access port to slot

**Explanation:** A robotic inject media operation returned a status indicating that an inject failure occurred.



**Recommended Action:**

- See whether the robotic library has a media access port (use the robot test utility to validate). Investigate whether the administrator or operator has canceled the inject operation.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Robotic status code 219

**Message:** Cannot move from slot to media access port

**Explanation:** A robotic eject media operation returned a status indicating that an eject failure occurred.

**Recommended Action:**

- See if the robotic library has a media access port (use the robot test utility to validate). Check if the administrator or operator has canceled the eject operation.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Robotic status code 220

**Message:** Media access port does not contain media

**Explanation:** A robotic inject media operation returned a status indicating that the media access port does not contain any cartridges/media. The operator or administrator may not have placed media into the media access port for inject.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Coordinate inject/eject operations between all of the operators and administrators.

## Robotic status code 221

**Message:** Media access port already contains media

**Explanation:** A robotic eject media operation returned a status indicating that the media access port contains one or more cartridges. The operator or administrator may not have removed the media from the media access port as part of the latest (or a previous) eject operation.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.
- Coordinate inject/eject operations between all operators and administrators. Ensure that the media access port is empty of media before an eject operation.

## Robotic status code 222

**Message:** Robotic arm has no addressable holder

**Explanation:** A holder is gone from an element of the robot and cannot be used.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the state of the physical hardware and correct the holder status for storage, drive, and transport elements as needed. Then, resubmit the request.

## Robotic status code 223

**Message:** Robot busy, cannot perform operation

**Explanation:** The robot is busy performing another operation, using resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing current external-based requests (including robot inventory and inject/eject media) before starting new requests. Check the vendor or operating system administrative interfaces and logs to see if the robotic resources are busy.

## Robotic status code 224

**Message:** Control daemon connect or protocol error

**Explanation:** A protocol error occurred between robotic and other components.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the system log messages that are related to the specific error leading to the media mount failure. Verify that all of the Media Manager binaries are at a compatible version level.
- Verify that the robotic interfaces to vendor and operating system software have compatible versions.

## Robotic status code 225

**Message:** Robot hardware or communication error

**Explanation:** A hardware or communications error occurred between robotic and other components.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Investigate the system log messages that are related to the error leading to the media mount failure.
- Verify that all of the Media Manager binaries are at a compatible version level. Verify that robotic interfaces to the vendor and operating system hardware and software have compatible versions.

## Robotic status code 226

**Message:** Requested slot contains the wrong tape

**Explanation:** The media in the requested slot is different from the media that is expected in that slot. The volume configuration is not consistent with the physical contents of the robotic library that is associated with the slot associated with the requested volume.

**Recommended Action:** The volume configuration or media placement in the robotic library needs to be adjusted using one of the media management interfaces. Determine whether the barcode changed or the media changed since the last time the EMM database was reconciled for the affected slot. If only the barcode has changed but not the media, issue an update barcode request for each affected

volume. If the media has been changed, use a media management interface to run robot inventory update, which updates the EMM database with the media location.

## Robotic status code 228

**Message:** Requested slot does not exist in robot

**Explanation:** The slot that is associated with a request is not valid for the robot.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Issue a robot inventory Contents report to determine the valid slot range for the robot. Check the volume configuration to ensure that only valid slots are referenced in volume records, paying particular attention to the starting and ending slot numbers. Update the volume configuration as needed, or request only valid slot ranges for robotic operations.

## Robotic status code 229

**Message:** Requested operation is not supported by the robot

**Explanation:** A robotic operation was either sent to a robotic component that did not support that operation, or the options that were requested for the operation were not supported. There may be an incompatibility between components or versions of the product.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that all of the Media Manager binaries and user interfaces are at a compatible version level.

## Robotic status code 230

**Message:** System error occurred during robot operation

**Explanation:** A robotic operation encountered a system error. This status code is used for generic system call failures within robotic daemons/processes.

**Recommended Action:**

- Check for other error messages in the command or interface output to indicate which system call failed. Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Check the system application log for error and warning messages.
- Verify that the system is not running out of virtual memory. If the virtual memory is the problem, shut down the unused applications or increase the amount of virtual memory. To increase the virtual memory on Windows: display the Control Panel, double-click **System**, and on the **Performance** tab, set Virtual Memory to a higher value.
- Verify that all of the product binaries are properly installed.
- Verify that no unexpected Media Manager processes are running by executing `vmps`. Some processes should remain running, but some processes that do not go away can indicate a problem, such as a hung system call.

## Robotic status code 232

**Message:** Volume not found in library

**Explanation:** The requested media was not found in the robotic library. The media has been ejected or become inaccessible for some other reason.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Issue a robot inventory Contents report to obtain the list of media in the robotic library. See if the inventory filters have been enabled in the Media Manager configuration file. Inventory filters affect the contents of the media list that was returned from the robotic daemon or process. Use a robot test utility or an operating system/vendor administrative interface to verify the status of the media, as needed. Update the volume configuration and search for the media if it was not in the robotic library, as needed, and resubmit the request.

## Robotic status code 233

**Message:** Volume is in library, but not in drive domain

**Explanation:** The media was in the robotic library, in a library domain that is inaccessible to the drives that are configured in the robot.

**Recommended Action:** Issue a robot inventory Contents report to obtain the list of media in the robotic library. Check the device configuration and ensure that the drive addresses correspond to the correct domain for the media. Correct the device configuration as needed and restart `ltid` (the device daemon on UNIX and Linux or NetBackup Device Manager service on Windows). Use a robot test utility or a vendor administrative interface to verify the status of media, as needed. Update the volume configuration and physically move the media into the robotic library, as needed, and resubmit the request.

## Robotic status code 234

**Message:** Robot denied access to the resource

**Explanation:** The media was found in the robotic library, but is denied access according to an established security policy.

**Recommended Action:** Issue a robot inventory Contents report to obtain the list of media in the robotic library. Use a vendor administrative interface to verify the status of media, as needed. Delete the media in the volume configuration, or make the volume accessible through a vendor administrative interface, as appropriate. Update the volume configuration, as needed, and resubmit the request.

## Robotic status code 235

**Message:** barcode label is unreadable

**Explanation:** The media was found in the robotic library, but it has an unreadable barcode label.

**Recommended Action:** Use the robot test utility or a vendor administrative interface to verify the status of the media. Correct the label or replace the media as appropriate. Update the volume configuration, as needed, and resubmit the request.

## Robotic status code 236

**Message:** Robot has misplaced the media

**Explanation:** The requested media was known, according to the vendor software managing the robotic library, but the media has been misplaced.

**Recommended Action:** Use a robot test utility or a vendor administrative interface to verify the status of media. Search for the media inside the robotic library. Update the volume configuration and search for the media if it was not in the robotic library, as needed, and resubmit the request.

## Robotic status code 237

**Message:** Volume is in use

**Explanation:** The media was in use.

**Recommended Action:** Use the robot test utility or a vendor administrative interface to verify the status of the media. Determine what applications may be using the media. Dismount the media if it is not being used. Wait for the media to become available, as needed.

## Robotic status code 238

**Message:** Requested drive is in an offline domain

**Explanation:** The drive that is targeted for a mount request was in a robotic library domain that is offline.

**Recommended Action:** Bring back the robotic library domain (ACS Library Storage Module) online, or postpone use of drives in that domain until the domain can be brought back online.

## Robotic status code 239

**Message:** Requested volume is in an offline domain

**Explanation:** The volume that is targeted for a mount request was in a robotic library domain that is in the offline or offline pending state.

**Recommended Action:** Bring back online the robotic library domain (ACS Library Storage Module), or postpone the use of media in that domain until the domain can be brought back online.

## Robotic status code 240

**Message:** A memory allocation attempt failed in the robotic daemon

**Explanation:** An attempt by the robotic control daemon to allocate memory has failed. This error may indicate serious memory problems on your media server.

**Recommended Action:** Stop all of the NetBackup Media Manager daemons. Consult the documentation for your operating system memory management tools to determine what remaining process is leaking memory, and stop that process. Restart the NetBackup Media Manager daemons. Free up memory by terminating the unneeded processes that consume a lot of memory. Add more swap space or physical memory, if necessary.

## Robotic status code 242

**Message:** Robot media access port does not exist

**Explanation:** The requested media access port was not valid for use with the targeted media.

**Recommended Action:** Use the robot test utility or a vendor administrative interface to verify the media access port address based on the location of the media. Choose a media access port that is valid, or let one be automatically selected, and retry the robotic operation.

## Robotic status code 243

**Message:** Cannot open/create the media access port status file

**Explanation:** A robotic daemon/process cannot create or open a status file in the database directory/folder.

**Recommended Action:** Investigate why the robot status file in the directory `/usr/opensv/volmgr/database` (UNIX and Linux) or folder `install_path\Volmgr\database` (Windows) cannot be created or opened. On Windows, check which account the NetBackup Device Manager service (and therefore, the robotic process) is running under. Compare it against the security properties of the database folder.

## Robotic status code 244

**Message:** The eject command was aborted by the user

**Explanation:** An administrator or operator canceled an eject media request.

**Recommended Action:** This error happens when an administrator or operator cancels an eject request. The request may have been canceled for the following reasons: missing or faulty media, to allow the media access port to be used for other requests, or to perform the operation at a later time. Check with the administrator or operator for more information.

## Robotic status code 245

**Message:** Physical drive is not available

**Explanation:** A robotic mount operation could not be completed because the physical drive resources are not available for the request. This error may result from an environment that is based on virtualized resources, such as one involving the Storagenet 6000 Storage Domain Manager (SN6000).



The SN6000 virtualizes tape drives. Some SN6000 configurations may have more logical drives than the number of physical drives (or equivalent resources) available for drive requests. Also, the relationship between the number of logical drives and physical drives may change as hardware failures occur. NetBackup scheduling, drive allocation, and drive assignment algorithms can only determine logical drive availability. NetBackup attempts to fully use all configured and available logical drives. If the number of required logical drives exceeds the physical drives available, a NetBackup job may be started with insufficient drive resources. Instead of queueing the job in the scheduler, the job runs and encounters the resource issue when it makes an ACS tape mount request.

**Recommended Action:**

- Install the Shared Storage Option (SSO) license for mount requests to requeue when physical drive resources are not available.
- The number of drives that can be in use at any one time is limited. Configure backup windows so the different storage units that are tied to the same physical drives are active only at non-overlapping times. Increase the media mount timeout to avoid job failures when the job cannot get a physical drive due to the drives all being busy.

## Robotic status code 246

**Message:** Failed to find an available slot to inject to

**Explanation:** An attempt to inject a volume into a full library failed. This error should only occur when the library is full. Full means that all storage elements either contain media or have been assigned media that are currently mounted in a drive. Note that some libraries that support multiple media types restrict which type of media can be assigned to each storage element. In this case, this error might occur even if some of the storage elements in a library were not full. Since the empty storage elements may not match the media type for the media to inject, the library is full for this media type.

**Recommended Action:** Clear the media access port, then re-inventory the robot by doing a volume configuration update.

## Robotic status code 249

**Message:** Volume is in home slot

**Explanation:** The volume is currently in its home slot and ready for eject.

**Recommended Action:** None

## Robotic status code 250

**Message:** Media access port is available

**Explanation:** The media access port is available for inject or eject.

**Recommended Action:** Begin the inject or eject operation.

## Robotic status code 251

**Message:** Media access port is unavailable

**Explanation:** The media access port is not ready for inject or eject.

**Recommended Action:** Manually remove any media remaining in the robot's media access port. If this status persists, check the robotic console for errors.

## Robotic status code 252

**Message:** Media access port is in inject mode

**Explanation:** The media access port is ready to inject and is not available for eject.

**Recommended Action:** Complete the inject operation.

## Robotic status code 253

**Message:** Media access port is in eject mode

**Explanation:** The media access port is ready to eject and is not available for inject.

**Recommended Action:** Complete the eject operation.

## Robotic status code 254

**Message:** Robot busy, inventory operation in progress

**Explanation:** The robot is not available because it is performing an inventory, using resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the inventory before you start new requests. Check the vendor or operating system administrative interfaces and logs to see if the robotic resources are busy.

## Robotic status code 255

**Message:** Robot busy, inject operation in progress

**Explanation:** The robot is not available because it is involved in an inject operation, using the resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the inject operation before you start new requests. Check the vendor or operating system administrative interfaces and logs to see if the robotic resources are busy.

## Robotic status code 256

**Message:** Robot busy, multiple eject operation in progress

**Explanation:** The robot is unavailable because a multiple eject is in progress, using the resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the multiple eject operation before you start new requests. Check the vendor or operating system administrative interfaces and logs to see if the robotic resources are busy.

## Robotic status code 257

**Message:** Robot busy, multiple inject operation in progress

**Explanation:** The robot is unavailable because a multiple inject is in progress, using the resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the multiple inject operation before you start new requests. Check the vendor or operating system administrative interfaces and logs to see if the robotic resources are busy.

## Robotic status code 258

**Message:** Cleaning/unknown media in drive

**Explanation:** A request to mount a tape failed because the cleaning media was found in the drive.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation once the drive cleaning has completed.

## Robotic status code 259

**Message:** Not authorized by VxSS

**Explanation:** A request was made to the robot daemons by an unauthorized user.

**Recommended Action:**

- Verify that the user has the necessary permissions to perform this operation.
- Verify that the authentication and authorization security settings are correct, under **Host Properties** in the **NetBackup Administration Console**. Information is available at the following location on how to use the Veritas Product Authentication and Authorization Service:  
 See the [NetBackup Security and Encryption Guide](#).

## Robotic status code 260

**Message:** Robot busy, robot diagnostics in progress

**Explanation:** The requested robot is running a robot diagnostic.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Retry the operation when the robot diagnostic cycle is complete.

## Robotic status code 261

**Message:** EMM error

**Explanation:** A request that was made to read/write data to EMM failed.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively processing commands.

## Robotic status code 262

**Message:** Configuration has changed, robot daemons and ltid need restarting

**Explanation:** A device configuration change has been made that is not reflected in the robotic daemon's run-time cache of the data.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Restart `ltid` and the robotics on this system or on the robot control host system.

# Robotic error codes

This chapter includes the following topics:

- [Robotic error codes](#)

## Robotic error codes

These status codes are returned if a robotic daemon/process was started from the command line and an error occurs. For example, if the administrator executes the following:

```
/usr/openv/volmgr/bin/tl8d
```

and no robots are configured, the following may be returned:

```
TL8: No robots are configured
```

These status codes are also logged to the system log.

Usually, robotic daemons/processes are not started from the command line, but are started automatically, as needed, when `ltid` starts.

### Robot Error status code 1

**Message:** You must be ROOT to start daemon

**Explanation:** A user other than root started a robotic daemon. This status only applies to UNIX and Linux systems.

**Recommended Action:** Log on as the root user before you start the robotic daemons. Allow the robotic daemons to be started automatically as needed by `ltid` (the device daemon).

## Robot Error status code 2

**Message:** LTI Daemon may not be running

**Explanation:** On an attempt to start a robotic daemon or process, the attempt to connect to the `ltid` message queue failed. This error indicates that `ltid` (the device daemon or NetBackup Device Manager service) may not be running.

**Recommended Action:**

- Start `ltid` so that the shared memory can be initialized, allowing the robotic daemon/process to function.
- If problems persist, examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see the resources that are currently in use.

## Robot Error status code 3

**Message:** Error in getting shared memory

**Explanation:** A robotic daemon/process was unable to get a shared memory identifier associated with the segment of shared memory that `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see the resources that are currently in use.

## Robot Error status code 4

**Message:** Error in attaching the shared memory

**Explanation:** A robotic daemon/process was unable to attach the shared memory segment that `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
 See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see the resources that are currently in use.

## Robot Error status code 5

**Message:** Error in getting process ID

**Explanation:** A robotic daemon/process was unable to obtain its own process identifier due to a system call failure.

**Recommended Action:** Investigate the operating system functionality regarding a process obtaining its own process identifier.

## Robot Error status code 6

**Message:** No devices are configured on the robot

**Explanation:** A robotic daemon/process was started, but no drives are configured for the robot.

**Recommended Action:** Some robotic daemons or processes do not run if there are not any drives configured for them to manage. Add or reconfigure one or more drives to be in the associated robot. Then, stop and restart `ltid` (the Media Manager device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).

## Robot Error status code 7

**Message:** No robots are configured

**Explanation:** A robotic daemon/process was started, but no robots of the associated robot type are configured.

**Recommended Action:** The robotic daemons or processes do not run if there are not any robots configured for the associated robot type. Add or reconfigure the robots, then stop and restart `ltid` (the Media Manager device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).



## Robot Error status code 8

**Message:** No memory available

**Explanation:** A robotic daemon/process was unable to allocate memory. This error occurs when insufficient system memory is available. This error can result from the system being overloaded with too many processes and from insufficient physical and virtual memory.

**Recommended Action:** Free up memory by terminating any unneeded processes. Add more swap space or physical memory.

## Robot Error status code 9

**Message:** Error in SEMAPHORE operation

**Explanation:** A process was unable to perform a semaphore operation (such as lock or unlock) associated with the resources maintained by `ltid`. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see the resources that are currently in use.

## Robot Error status code 10

**Message:** Fork failure occurred

**Explanation:** A robotic daemon or process cannot create a child process due to a system error. This error is probably intermittent, based on the availability of resources on the system (only applies to UNIX and Linux servers).

**Recommended Action:**

- Restart the device daemon at a later time and investigate the system problems that limit the number of processes.
- Examine the system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

- Restart the device daemon, then retry the operation and examine the system log file.

## Robot Error status code 11

**Message:** System error occurred

**Explanation:** A robotic daemon/process encountered a system error.

**Recommended Action:** Examine the command output, debug logs, and system logs for a more detailed message on the error.

See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Robot Error status code 12

**Message:** Usage error in creating child process

**Explanation:** A robotic daemon/process cannot create a child process due to an incompatibility between robotic software components.

**Recommended Action:**

- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).
- Verify that all of the Media Manager binaries are at a compatible version level.

## Robot Error status code 13

**Message:** EMM error

**Explanation:** The robotic daemon had a problem communicating with EMM.

**Recommended Action:**

- Make sure `nbemm` is running and responding to requests.
- Examine the command output, debug logs, and system logs for a more detailed message on the error.  
See "Setting Media Manager debug logging to a higher level" in the [NetBackup Logging Reference Guide](#).

## Robot Error status code 14

**Message:** You must be an administrator to execute

**Explanation:** A robotic process was started under a user account that lacks Administrator privileges (only applies to Windows systems).

**Recommended Action:** Allow the robotic daemons to be started automatically as needed by the NetBackup Device Manager service. Ensure that this service starts from a user account with administrator privileges.

## Robot Error status code 16

**Message:** Devices located in multiple domains

**Explanation:** A robotic daemon or process encountered an invalid device configuration. In this configuration, a single logical robot controls drives from different domains.

**Recommended Action:** Display the device configuration using `tpconfig -d` or a device configuration interface to see the robotic and the drive information that is already configured. Ensure that the drive addresses do not span physical domains. Drives can only be configured in the same robot if they can be used with media from a single domain. The domain must include a single physical library or multiple libraries that are connected by a cartridge exchange or pass-through mechanism.

## Robot Error status code 17

**Message:** Robotic daemon not licensed

**Explanation:** A robotic daemon or process was started without the required, current product license, or a required database file was missing or corrupt.

**Recommended Action:**

- Check product documentation for supported device configurations.
- Obtain an additional software license that allows robots of the associated robot type to be configured. Or, limit the configuration to the robot types that current licensing allows. Check for the existence and permissions of the `external_robotics.txt` file in the `/usr/openv/share` directory (UNIX and Linux) or in the `install_path\NetBackup\share` folder (Windows).

# Security services status codes

This chapter includes the following topics:

- [Security services status codes](#)

## Security services status codes

The security services status codes appear in the exit status and command output for the `bpnbat` command when you authenticate a user with the NetBackup authentication daemon (`nbatd`) or the NetBackup web service (`nbwmc`) to get a user certificate or a session token.

### Security services status code 93

**Message:** Web authentication failed.

**Explanation:** Web authentication has failed.

**Recommended Action:** Either the user name, domain name, domain type, or password is incorrect. Check the user authorization permission. Check the `bpnbat` logs for further diagnostics.

### Security services status code 94

**Message:** Both AT authentication and Web authentication failed.

**Explanation:** Authentication for the NetBackup AT broker and the web application has failed.

**Recommended Action:** Ensure that both the NetBackup web service (`nbwmc`) and the NetBackup authentication daemon (`nbatd`) are running on the master server.

Either the user name, domain name, domain type, or password is incorrect. Check the `bpnbat` logs for further diagnostics.

## Security services status code 95

**Message:** AT authentication successful, web authentication failed.

**Explanation:** When the login type is not specified, both the NetBackup AT broker and the NetBackup web application logins are performed. However, authentication for the NetBackup web application has failed.

**Recommended Action:** Ensure that the NetBackup web service (`nbwmc`) is running on the master server. Check the `bpnbat` logs for further diagnostics.

## Security services status code 96

**Message:** Web authentication successful, AT authentication failed.

**Explanation:** When the login type is not specified, both the NetBackup AT broker and the NetBackup web application logins are performed. However, authentication for the NetBackup AT broker has failed.

**Recommended Action:** Ensure that the NetBackup authentication daemon (`nbatd`) is running on the master server. Check the `bpnbat` logs for further diagnostics.

## Security services status code 97

**Message:** Web logout failed.

**Explanation:** The logout operation to the NetBackup web application failed.

**Recommended Action:** Ensure that the NetBackup web service (`nbwmc`) is running on the master server.

## Security services status code 98

**Message:** Web logout was successful, but the AT logout failed.

**Explanation:** When the logout type is not specified, both the NetBackup AT broker and the web application logouts are performed. However, the NetBackup authentication broker logout failed.

**Recommended Action:** Retry the operation. If the problem continues, save all of the error log information and call Veritas Technical Support.

## Security services status code 99

**Message:** AT logout was successful, but the web logout failed.

**Explanation:** When the logout type is not specified, both the NetBackup AT broker and the web application logouts are performed. However, the NetBackup web application logout failed.

**Recommended Action:** Ensure that the NetBackup web service (`nbwmc`) is running on the master server.

## Security services status code 100

**Message:** Both the AT and the web logout failed.

**Explanation:** The NetBackup AT broker and the web application logout failed.

**Recommended Action:** Ensure that the NetBackup web service (`nbwmc`) is running on the master server and retry the operation.

## Security services status code 101

**Message:** The CA certificate is not present or is invalid.

**Explanation:** The NetBackup web login or logout failed because the NetBackup web authentication services' certificate could not be verified using a CA certificate from the local trust store.

**Recommended Action:** Run the `nbcertcmd -getCACertificate` command to get a new CA certificate and try again. You can also run the `nbcertcmd -listCACertDetails` command to list the CA certificates that are in the local trust store. Ensure that the NetBackup web service (`nbwmc`) is running on the master server and retry the operation.

## Security services status code 102

**Message:** Unable to connect to the NetBackup web authentication service.

**Explanation:** The NetBackup web login or logout failed because NetBackup cannot connect to the web authentication service.

**Recommended Action:** Ensure that the NetBackup web service (`nbwmc`) is running on the master server.

## Security services status code 103

**Message:** Unable to send information to the NetBackup web authentication service.

**Explanation:** The NetBackup web login or logout failed because NetBackup cannot send information to the NetBackup web authentication service.

**Recommended Action:** Check if the NetBackup web service (`nbwmc`) is running and restart it, if required.

## Security services status code 104

**Message:** Unable to read information from the NetBackup web authentication service.

**Explanation:** The NetBackup web login or logout failed because NetBackup cannot read the token information from the NetBackup web authentication service.

**Recommended Action:** Check if the NetBackup web service (`nbwmc`) is running and restart it, if required.

## Security services status code 105

**Message:** Unable to retrieve user authentication details on the current host.

**Explanation:** The user authentication details from the NetBackup web login cannot be retrieved on the current host.

**Recommended Action:** Try to log in again with the `bpnbat -login` command. If the problem continues, save all of the error log information and contact Veritas Technical Support.

## Security services status code 106

**Message:** Authentication successful but unable to store the user details on the current host.

**Explanation:** The NetBackup web login authentication succeeded, but the user details were not stored on the current host.

**Recommended Action:** Try to log in again with the `bpnbat -login` command. If the problem continues, save all of the error log information and contact Veritas Technical Support.

## Security services status code 107

**Message:** Failed to get logged in user details; either the credentials are expired or are not available.

**Explanation:** The `bpnbat -whoami` command returns this error when it does not find the AT credentials and web token.

**Recommended Action:** Try to log in again with the `bpnbat -login` command. If the problem continues, save all of the error log information and contact Veritas Technical Support.