

# **Provisioning Manager and Protection Manager Printable Help**

For Use with DataFabric Manager® Server 3.8

NetApp, Inc.  
495 East Java Drive  
Sunnyvale, CA 94089 USA  
Telephone: +1 (408) 822-6000  
Fax: +1 (408) 822-4501  
Support telephone: +1 (888) 4-NETAPP  
Documentation comments: [doccomments@netapp.com](mailto:doccomments@netapp.com)  
Information Web: <http://www.netapp.com>  
Part number: 215-04723\_A0



# Contents

<b>About this document.....</b>	<b>17</b>
<b>Welcome to NetApp Management Console Help.....</b>	<b>19</b>
<b>Copyright information.....</b>	<b>21</b>
<b>Trademark information.....</b>	<b>23</b>
<b>Contact information.....</b>	<b>25</b>
<b>What NetApp Management Console is.....</b>	<b>27</b>
<b>Applications that run in NetApp Management Console .....</b>	<b>29</b>
<b>NetApp Management Console window layout and navigation.....</b>	<b>31</b>
<b>NetApp Management Console window customization.....</b>	<b>33</b>
<b>NetApp Management Console data filtering.....</b>	<b>35</b>
<b>Notifications.....</b>	<b>37</b>
<b>Descriptions of severity types.....</b>	<b>39</b>
<b>How to know when an event occurs.....</b>	<b>41</b>
<b>List of events and severity types.....</b>	<b>43</b>
<b>Monitoring events.....</b>	<b>65</b>
<b>Responding to and acknowledging events.....</b>	<b>67</b>
<b>Deleting events.....</b>	<b>69</b>
<b>What alarms are.....</b>	<b>71</b>
<b>Differences between alarms and user alerts.....</b>	<b>73</b>
<b>Alarms triggered from related objects .....</b>	<b>75</b>
<b>Guidelines for using alarms.....</b>	<b>77</b>
<b>Alarm properties.....</b>	<b>79</b>
<b>Decisions to make before adding an alarm .....</b>	<b>83</b>
<b>Adding alarms.....</b>	<b>85</b>
<b>Testing alarms.....</b>	<b>87</b>
<b>Editing alarms.....</b>	<b>89</b>
<b>Deleting alarms.....</b>	<b>91</b>
<b>Overview of alarm management tasks.....</b>	<b>93</b>
Typical alarm management tasks.....	93

Infrequent alarm management tasks.....	94
<b>Responding to alarms.....</b>	<b>95</b>
Monitoring alarms.....	97
Enabling and disabling alarms.....	99
Role-based access control (RBAC).....	101
Administrator roles and capabilities.....	103
Viewing NetApp Management Console configuration and licensing details.....	109
Printing Help topics.....	111
About the NetApp Management Console dashboards.....	127
Dashboard panel descriptions.....	129
How hosts become visible to the console.....	133
Ways to investigate problems with hosts.....	135
Data ONTAP licenses used for protecting or provisioning data.....	137
When qtree SnapMirror is used to perform backups.....	141
How to customize a vFiler unit configuration using a script.....	143
Decisions to make before adding a storage system.....	145
Adding a storage system.....	147
Decisions to make before adding an Open Systems SnapVault host.....	149
Guidelines for adding and editing an Open Systems SnapVault host on an ESX server.....	151
Adding an Open Systems SnapVault host.....	153
Decisions to make before adding a vFiler unit.....	155
Adding a vFiler unit.....	159
Decisions to make before setting up vFiler unit properties.....	161
Considerations for active/active hosts.....	165
Setting up vFiler unit properties.....	167
Editing storage system properties.....	169
Editing Open Systems SnapVault properties.....	171
Stopping Open Systems SnapVault agents.....	173
Starting Open Systems SnapVault agents.....	175

<b>Updating Open Systems SnapVault client data.....</b>	<b>177</b>
<b>Diagnosing a storage system.....</b>	<b>179</b>
<b>Diagnosing an Open Systems SnapVault host.....</b>	<b>181</b>
<b>vFiler unit migration overview.....</b>	<b>183</b>
<b>vFiler unit migration requirements.....</b>	<b>185</b>
<b>Description of migration tasks.....</b>	<b>187</b>
Migration Step 1. Start.....	188
Migration Step 2. Update (optional).....	188
Migration Step 3. Cutover.....	189
Migration Step 4. Cleanup.....	190
Manual cleanup after migration.....	190
<b>Decisions to make before starting vFiler unit migration.....</b>	<b>191</b>
<b>Starting a vFiler unit migration.....</b>	<b>193</b>
<b>Updating vFiler unit migration SnapMirror relationships.....</b>	<b>195</b>
<b>Cutting over to the new vFiler unit destination.....</b>	<b>197</b>
<b>Cleaning up a vFiler unit migration.....</b>	<b>199</b>
<b>Canceling a vFiler unit migration.....</b>	<b>201</b>
<b>Viewing vFiler unit migration status.....</b>	<b>203</b>
<b>Overview of resource pools.....</b>	<b>205</b>
<b>Advantages of using resource pools.....</b>	<b>207</b>
<b>Resource pool properties.....</b>	<b>209</b>
<b>Ways you might combine resources in resource pools.....</b>	<b>211</b>
<b>Sequence for selecting backup destination volumes.....</b>	<b>213</b>
<b>Sequence for selecting mirror destination volumes.....</b>	<b>215</b>
<b>Resource pool guidelines.....</b>	<b>217</b>
<b>How resource labels work.....</b>	<b>221</b>
<b>Decisions to make before adding a resource pool.....</b>	<b>223</b>
<b>Adding a resource pool.....</b>	<b>227</b>
<b>Impact of modifying resource pool properties.....</b>	<b>229</b>
<b>Editing resource pool properties.....</b>	<b>231</b>
<b>What a protection policy is .....</b>	<b>233</b>
<b>Types of data protection .....</b>	<b>235</b>
Local backup protection.....	235

Remote backup protection.....	235
Mirror protection.....	236
<b>Protection policy nodes and connections.....</b>	<b>237</b>
<b>Protection policies (not disaster recovery capable).....</b>	<b>239</b>
<b>Retention of hourly, daily, weekly, and monthly backups .....</b>	<b>241</b>
Backup retention strategies .....	241
Backup retention classes.....	242
<b>Protection policy node prerequisites.....</b>	<b>243</b>
<b>Allowable lag times.....</b>	<b>247</b>
<b>Protection schedules and time zones.....</b>	<b>249</b>
<b>Decisions to make before adding a protection policy.....</b>	<b>251</b>
<b>Adding a protection policy.....</b>	<b>255</b>
<b>Editing a protection policy.....</b>	<b>257</b>
Editing a policy's primary data node.....	258
Editing a policy's backup connection.....	259
Editing a policy's backup node.....	260
Editing a policy's mirror connection.....	260
Editing a policy's mirror node.....	261
<b>Assigning or changing schedules in a protection policy.....</b>	<b>263</b>
<b>Changing retention times in a protection policy.....</b>	<b>265</b>
<b>Changing lag thresholds in a protection policy.....</b>	<b>267</b>
<b>Changing a node name in a policy.....</b>	<b>269</b>
<b>Deleting a protection policy.....</b>	<b>271</b>
<b>Effect of time zones on schedules.....</b>	<b>273</b>
Ways to set the time zone.....	274
Guidelines for using time zones with resource pools.....	276
Guidelines for using time zones with datasets.....	277
<b>Example of a schedule using local time zones.....</b>	<b>279</b>
Time zone assignment (local).....	279
Time zone selection for protection schedules (local).....	280
Results of scheduled jobs (local).....	281
<b>Example of a schedule using a default time zone.....</b>	<b>283</b>
Time zone assignment (default).....	283
Time zone selection for protection schedules (default).....	284

Results of scheduled jobs (default).....	285
<b>Types of schedules.....</b>	<b>287</b>
<b>Summary of schedule features.....</b>	<b>289</b>
<b>Configuration sequence for schedules, policies, and datasets.....</b>	<b>291</b>
<b>Planning schedules for protection policy nodes and connections.....</b>	<b>293</b>
Planning a schedule for the primary data node.....	293
Planning a schedule for a backup connection.....	294
Planning a schedule for a mirror connection.....	294
<b>Description of daily, weekly, and monthly protection schedules.....</b>	<b>295</b>
<b>Throttle schedules and network bandwidth.....</b>	<b>297</b>
<b>Throttle schedule properties.....</b>	<b>299</b>
<b>Protection schedules and time zones.....</b>	<b>301</b>
<b>Decisions to make before adding a schedule .....</b>	<b>303</b>
<b>Adding a daily protection schedule.....</b>	<b>307</b>
<b>Adding a weekly protection schedule.....</b>	<b>309</b>
<b>Adding a monthly protection schedule.....</b>	<b>311</b>
<b>Adding a throttle schedule.....</b>	<b>313</b>
<b>Editing a daily schedule.....</b>	<b>315</b>
<b>Editing a weekly schedule.....</b>	<b>317</b>
<b>Editing a monthly schedule.....</b>	<b>319</b>
<b>Editing a throttle schedule.....</b>	<b>321</b>
<b>Deleting a protection or throttle schedule.....</b>	<b>323</b>
<b>Assigning or changing schedules in a protection policy.....</b>	<b>325</b>
<b>Copying a protection or throttle schedule.....</b>	<b>327</b>
<b>Dataset concepts.....</b>	<b>329</b>
<b>How the protection application uses datasets.....</b>	<b>331</b>
<b>How the provisioning application works with datasets.....</b>	<b>333</b>
<b>About NFS, CIFS, iSCSI, or FC protocol access .....</b>	<b>335</b>
<b>When to configure datasets.....</b>	<b>337</b>
<b>How to enable backup of multiple primary volumes to a single secondary volume.....</b>	<b>339</b>
<b>Dataset storage space management.....</b>	<b>341</b>
When to manually manage storage space for a dataset.....	341

How to view dataset storage space utilization.....	342
Overview of tasks for managing storage space.....	342
Space management resize options.....	343
<b>Dataset properties.....</b>	<b>345</b>
<b>Decisions to make before adding datasets.....</b>	<b>347</b>
Dataset protection decisions.....	347
Dataset provisioning decisions.....	350
Custom name prefixes for dataset volumes, qtrees, and Snapshot copies.....	352
<b>Adding a dataset.....</b>	<b>355</b>
<b>Decisions to make before assigning or changing policies.....</b>	<b>357</b>
<b>Assigning or changing a protection policy.....</b>	<b>361</b>
<b>Assigning or changing a provisioning policy.....</b>	<b>363</b>
<b>Decisions to make before provisioning a dataset.....</b>	<b>365</b>
<b>Provisioning resources for a primary dataset node.....</b>	<b>367</b>
<b>How to select a specific aggregate or storage system for provisioning.....</b>	<b>369</b>
<b>Decisions to make before adding or changing resource assignments.....</b>	<b>371</b>
<b>Adding resources to a dataset.....</b>	<b>373</b>
<b>Changing dataset node resource assignments.....</b>	<b>375</b>
<b>Removing resources from a dataset.....</b>	<b>377</b>
<b>Overview of export protocol properties.....</b>	<b>379</b>
<b>Configuring dataset nodes for CIFS protocol access .....</b>	<b>381</b>
<b>Configuring dataset nodes for NFS protocol access .....</b>	<b>383</b>
<b>Configuring dataset nodes for FC protocol access.....</b>	<b>385</b>
<b>Configuring dataset nodes for iSCSI protocol access .....</b>	<b>387</b>
<b>Editing dataset general properties.....</b>	<b>389</b>
<b>Deleting a dataset.....</b>	<b>391</b>
<b>Overview of managing protected data.....</b>	<b>393</b>
Description of dataset protection status.....	394
Description of dataset conformance status.....	395
Description of dataset resource status.....	395
<b>How to evaluate dataset conformance to policy.....</b>	<b>397</b>
Why datasets fail to conform to policy .....	397

How the protection application monitors dataset conformance.....	397
Dataset conformance conditions.....	399
<b>Monitoring dataset status.....</b>	<b>403</b>
<b>Monitoring backup and mirror relationships.....</b>	<b>405</b>
<b>Backing up datasets on-demand.....</b>	<b>407</b>
<b>Suspending protection of datasets.....</b>	<b>409</b>
<b>Suspending data protection for backup volume maintenance.....</b>	<b>411</b>
<b>Resuming protection of datasets.....</b>	<b>413</b>
<b>Displaying export and mapping information for all members of a dataset node.....</b>	<b>415</b>
<b>Displaying export properties for a specific dataset member.....</b>	<b>417</b>
<b>Overview of restoring data.....</b>	<b>419</b>
Restore guidelines.....	421
The restore_symboltable file.....	421
<b>Restoring backed-up data to a new location.....</b>	<b>423</b>
<b>Restoring backed-up data over current data.....</b>	<b>425</b>
<b>Restoring selected portions of a dataset.....</b>	<b>427</b>
<b>Restoring a virtual machine to its original location.....</b>	<b>429</b>
<b>Restoring a virtual machine file system to any location.....</b>	<b>431</b>
<b>Restoring a virtual machine to its original location through another ESX server.....</b>	<b>433</b>
<b>About unprotected data.....</b>	<b>435</b>
<b>Where to view unprotected data.....</b>	<b>437</b>
<b>Hosts that contain unprotected data.....</b>	<b>439</b>
<b>When to import discovered relationships.....</b>	<b>441</b>
<b>Adding unprotected host data to an existing dataset.....</b>	<b>443</b>
<b>Adding unprotected host data to a new dataset.....</b>	<b>445</b>
<b>Protecting unprotected datasets.....</b>	<b>447</b>
<b>Decisions to make before importing external relationships.....</b>	<b>449</b>
<b>Importing discovered external relationships.....</b>	<b>451</b>
<b>What groups are.....</b>	<b>453</b>
<b>What the global group is.....</b>	<b>455</b>
<b>Group properties.....</b>	<b>457</b>

<b>Decisions to make before adding groups.....</b>	<b>459</b>
<b>Adding groups.....</b>	<b>461</b>
<b>Editing groups .....</b>	<b>463</b>
<b>Deleting groups.....</b>	<b>465</b>
<b>Monitoring jobs.....</b>	<b>467</b>
<b>Cancelling jobs.....</b>	<b>469</b>
<b>Where to view reports and logs.....</b>	<b>471</b>
<b>What disaster recovery protection is.....</b>	<b>623</b>
When you use disaster recovery .....	623
Recovery strategies after failover .....	624
Disaster recovery protection tasks.....	624
<b>Disaster recovery concepts.....</b>	<b>625</b>
<b>Disaster recovery capable protection policies.....</b>	<b>627</b>
<b>Protection policy node prerequisites.....</b>	<b>629</b>
<b>Volumes unsuitable as mirror destinations .....</b>	<b>633</b>
<b>What happens during failover .....</b>	<b>635</b>
<b>What failover scripts are.....</b>	<b>637</b>
Failover script variables.....	637
Failover script example.....	638
<b>Decisions to make before configuring disaster recovery protection.....</b>	<b>639</b>
Disaster recovery capable dataset considerations.....	639
Disaster recovery protection policy considerations .....	640
<b>Enabling disaster recovery protection.....</b>	<b>641</b>
<b>Ensuring disaster recovery readiness.....</b>	<b>643</b>
Monitoring failover readiness.....	643
Testing failover scripts.....	644
<b>Executing disaster procedures.....</b>	<b>645</b>
Disaster management options.....	645
Updating disaster recovery node storage before failover.....	646
Starting failover.....	647
Monitoring failover status.....	648
<b>Recovery from disaster.....</b>	<b>649</b>
Making the disaster recovery node the new primary data storage.....	649
Recovering by resuming forward mirroring.....	651

Recovering by resynchronizing data to undestroyed containers.....	652
Recovering by resynchronizing data to replaced containers .....	654
<b>What Provisioning Manager is.....</b>	<b>685</b>
<b>About the NetApp Management Console dashboards.....</b>	<b>687</b>
<b>Dashboard panel descriptions.....</b>	<b>689</b>
<b>Dataset concepts.....</b>	<b>693</b>
<b>How the protection application uses datasets.....</b>	<b>695</b>
<b>How the provisioning application works with datasets.....</b>	<b>697</b>
<b>About NFS, CIFS, iSCSI, or FC protocol access .....</b>	<b>699</b>
<b>When to configure datasets.....</b>	<b>701</b>
<b>How to enable backup of multiple primary volumes to a single secondary volume.....</b>	<b>703</b>
<b>Dataset storage space management.....</b>	<b>705</b>
When to manually manage storage space for a dataset.....	705
How to view dataset storage space utilization.....	706
Overview of tasks for managing storage space.....	706
Space management resize options.....	707
<b>Dataset properties.....</b>	<b>709</b>
<b>Decisions to make before adding datasets.....</b>	<b>711</b>
Dataset protection decisions.....	711
Dataset provisioning decisions.....	714
Custom name prefixes for dataset volumes, qtrees, and Snapshot copies.....	716
<b>Adding a dataset.....</b>	<b>719</b>
<b>Decisions to make before assigning or changing policies.....</b>	<b>721</b>
<b>Assigning or changing a protection policy.....</b>	<b>725</b>
<b>Assigning or changing a provisioning policy.....</b>	<b>727</b>
<b>Decisions to make before provisioning a dataset.....</b>	<b>729</b>
<b>Provisioning resources for a primary dataset node.....</b>	<b>731</b>
<b>How to select a specific aggregate or storage system for provisioning.....</b>	<b>733</b>
<b>Decisions to make before adding or changing resource assignments....</b>	<b>735</b>
<b>Adding resources to a dataset.....</b>	<b>737</b>
<b>Changing dataset node resource assignments.....</b>	<b>739</b>

<b>Removing resources from a dataset.....</b>	<b>741</b>
<b>Overview of export protocol properties.....</b>	<b>743</b>
<b>Configuring dataset nodes for CIFS protocol access .....</b>	<b>745</b>
<b>Configuring dataset nodes for NFS protocol access .....</b>	<b>747</b>
<b>Configuring dataset nodes for FC protocol access.....</b>	<b>749</b>
<b>Configuring dataset nodes for iSCSI protocol access .....</b>	<b>751</b>
<b>Editing dataset general properties.....</b>	<b>753</b>
<b>Deleting a dataset.....</b>	<b>755</b>
<b>Viewing volume, LUN or qtree space allocation.....</b>	<b>757</b>
<b>Diagnosing volume or qtree space status.....</b>	<b>759</b>
<b>Resizing volume space.....</b>	<b>761</b>
<b>Resizing qtree space.....</b>	<b>763</b>
<b>Deleting Snapshot copies.....</b>	<b>765</b>
<b>Deleting a volume, LUN or qtree.....</b>	<b>767</b>
<b>Dataset migration overview.....</b>	<b>769</b>
<b>Dataset migration requirements.....</b>	<b>771</b>
<b>Dataset migration and failover.....</b>	<b>773</b>
<b>Dataset migration limitations.....</b>	<b>775</b>
<b>When to relinquish the migration capability of a dataset.....</b>	<b>777</b>
<b>Strategies for enabling a dataset for migration.....</b>	<b>779</b>
<b>Decisions to make before starting dataset migration.....</b>	<b>781</b>
<b>Starting a dataset migration.....</b>	<b>783</b>
<b>Updating dataset migration SnapMirror relationships.....</b>	<b>785</b>
<b>Cutting over to the new dataset storage destination.....</b>	<b>787</b>
<b>Cleaning up a dataset migration.....</b>	<b>789</b>
<b>Canceling a dataset migration.....</b>	<b>791</b>
<b>Viewing dataset migration status.....</b>	<b>793</b>
<b>Environment variables for data migration scripts.....</b>	<b>795</b>
<b>Relinquishing migration capability of a dataset.....</b>	<b>797</b>
<b>What deduplication is.....</b>	<b>799</b>
<b>Deduplication configuration requirements.....</b>	<b>801</b>
<b>What happens during deduplication.....</b>	<b>803</b>

<b>Over deduplication.....</b>	<b>805</b>
<b>Deduplication space savings percentage .....</b>	<b>807</b>
<b>Enabling deduplication on your dataset nodes.....</b>	<b>809</b>
<b>Disabling deduplication on dataset nodes.....</b>	<b>811</b>
<b>Starting on-demand deduplication.....</b>	<b>813</b>
<b>Stopping an in-progress deduplication .....</b>	<b>815</b>
<b>Viewing volume-level deduplication space-saving.....</b>	<b>817</b>
<b>Overview of resource pools.....</b>	<b>819</b>
<b>Advantages of using resource pools.....</b>	<b>821</b>
<b>Resource pool properties.....</b>	<b>823</b>
<b>Ways you might combine resources in resource pools.....</b>	<b>825</b>
<b>Sequence for selecting backup destination volumes.....</b>	<b>827</b>
<b>Sequence for selecting mirror destination volumes.....</b>	<b>829</b>
<b>Resource pool guidelines.....</b>	<b>831</b>
<b>How resource labels work.....</b>	<b>835</b>
<b>Decisions to make before adding a resource pool.....</b>	<b>837</b>
<b>Adding a resource pool.....</b>	<b>841</b>
<b>Impact of modifying resource pool properties.....</b>	<b>843</b>
<b>Editing resource pool properties.....</b>	<b>845</b>
<b>What a policy is.....</b>	<b>847</b>
What a protection policy is .....	847
What a provisioning policy is.....	848
<b>Difference between provisioning policy and provisioning wizard .....</b>	<b>851</b>
<b>Provisioning policy properties.....</b>	<b>853</b>
<b>Viewing a provisioning policy.....</b>	<b>859</b>
<b>Decisions to make before adding a provisioning policy .....</b>	<b>861</b>
Types of provisioning policies .....	863
What storage availability levels are.....	864
What RAID4 protection is.....	865
What RAID-DP protection is.....	865
What SyncMirror is.....	866
Advantages of using SyncMirror.....	866

What an active/active configuration is.....	866
Benefits of an active/active configuration.....	867
What a resource label is.....	867
Why you use quotas.....	867
Overview of the quota process.....	868
Quota targets and types.....	868
How space management works.....	869
What space guarantees are.....	869
What space reservation is.....	870
What fractional reserve is.....	871
Space utilization thresholds.....	872
What provisioning scripts are.....	873
<b>Adding a provisioning policy.....</b>	<b>875</b>
<b>Decisions to make before editing a provisioning policy .....</b>	<b>877</b>
<b>Editing a provisioning policy.....</b>	<b>879</b>
<b>Copying a provisioning policy.....</b>	<b>881</b>
<b>Deleting a provisioning policy.....</b>	<b>883</b>
<b>What vFiler templates are.....</b>	<b>885</b>
<b>vFiler template properties.....</b>	<b>887</b>
<b>Viewing vFiler templates.....</b>	<b>889</b>
<b>Decisions to make before adding vFiler templates.....</b>	<b>891</b>
<b>Adding a vFiler template.....</b>	<b>893</b>
<b>Editing a vFiler template.....</b>	<b>895</b>
<b>Copying a vFiler template.....</b>	<b>897</b>
<b>Deleting a vFiler template.....</b>	<b>899</b>
<b>How hosts become visible to the console.....</b>	<b>901</b>
<b>Ways to investigate problems with hosts.....</b>	<b>903</b>
<b>Data ONTAP licenses used for protecting or provisioning data.....</b>	<b>905</b>
<b>When qtree SnapMirror is used to perform backups.....</b>	<b>909</b>
<b>How to customize a vFiler unit configuration using a script.....</b>	<b>911</b>
<b>Decisions to make before adding a storage system.....</b>	<b>913</b>
<b>Adding a storage system.....</b>	<b>915</b>

<b>Decisions to make before adding an Open Systems SnapVault host.....</b>	<b>917</b>
<b>Guidelines for adding and editing an Open Systems SnapVault host on an ESX server.....</b>	<b>919</b>
<b>Adding an Open Systems SnapVault host.....</b>	<b>921</b>
<b>Decisions to make before adding a vFiler unit.....</b>	<b>923</b>
<b>Adding a vFiler unit.....</b>	<b>927</b>
<b>Decisions to make before setting up vFiler unit properties.....</b>	<b>929</b>
<b>Considerations for active/active hosts.....</b>	<b>933</b>
<b>Setting up vFiler unit properties.....</b>	<b>935</b>
<b>Editing storage system properties.....</b>	<b>937</b>
<b>Editing Open Systems SnapVault properties.....</b>	<b>939</b>
<b>Stopping Open Systems SnapVault agents.....</b>	<b>941</b>
<b>Starting Open Systems SnapVault agents.....</b>	<b>943</b>
<b>Updating Open Systems SnapVault client data.....</b>	<b>945</b>
<b>Diagnosing a storage system.....</b>	<b>947</b>
<b>Diagnosing an Open Systems SnapVault host.....</b>	<b>949</b>
<b>vFiler unit migration overview.....</b>	<b>951</b>
<b>vFiler unit migration requirements.....</b>	<b>953</b>
<b>Description of migration tasks.....</b>	<b>955</b>
Migration Step 1. Start.....	956
Migration Step 2. Update (optional).....	956
Migration Step 3. Cutover.....	957
Migration Step 4. Cleanup.....	958
Manual cleanup after migration.....	958
<b>Decisions to make before starting vFiler unit migration.....</b>	<b>959</b>
<b>Starting a vFiler unit migration.....</b>	<b>961</b>
<b>Updating vFiler unit migration SnapMirror relationships.....</b>	<b>963</b>
<b>Cutting over to the new vFiler unit destination.....</b>	<b>965</b>
<b>Cleaning up a vFiler unit migration.....</b>	<b>967</b>
<b>Canceling a vFiler unit migration.....</b>	<b>969</b>
<b>Viewing vFiler unit migration status.....</b>	<b>971</b>
<b>Monitoring jobs.....</b>	<b>973</b>

<b>Cancelling jobs.....</b>	<b>975</b>
<b>Where to view reports and logs.....</b>	<b>977</b>
<b>Index.....</b>	<b>1061</b>

# About this document

---

This document is a printable version of the NetApp Management Console Help for Protection Manager and Provisioning Manager. It is intended to be used for offline searches when you do not have access to the Help on a management station. The Help contains administrative tasks, as well as conceptual and reference material that can be useful in understanding how the protection and provisioning applications work.

**Note:** NetApp Management Console displays the portions of the Help that are appropriate for the licenses that are installed on the DataFabric Manager server. Because this document is static, it includes the entire help for the protection, disaster recovery, and provisioning licenses.

**Note:** Many Help topics occur in more than one place. For example, many of the topics about datasets and hosts occur in both the Protection Help and Provisioning Help sections. In dynamic Help, this structure increases usability by making information easier to find. In a static document, such as this one, this same structure can make searches more confusing, because a search might result in multiple hits to the same topic.



# Welcome to NetApp Management Console Help

---

This Help includes information for all applications installed on NetApp Management Console .

By using the table of contents and index or the search tool, you can find information about application features and how to use them. This Help is structured as follows:

- General information about NetApp Management Console and tools common to all applications installed on NetApp Management Console , such as alarms, events, and administrative user access (RBAC).
- Information about Protection Manager
- Information about Provisioning Manager
- Information about Performance Advisor

Help is also available from every window and its respective tabs. To learn about a specific window parameter, click  or click the Help menu in the task bar and select **Help For This View**.

You can also print selected Help topics.

## Related concepts

[NetApp Management Console window layout and navigation](#) on page 31

## Related tasks

[Printing Help topics](#) on page 111



# Copyright information

---

Copyright © 1994–2009 NetApp, Inc. All rights reserved. Printed in the U.S.A.

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

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

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

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

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

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



# Trademark information

---

All applicable trademark attribution is listed here.

NetApp, the Network Appliance logo, the bolt design, NetApp-the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; Serving Data by Design; Shadow Tape; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; VFM Virtual File Manager; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

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

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

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

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetCache is certified RealSystem compatible.



# Contact information

---

Information about how to contact NetApp is listed here.

NetApp, Inc.

495 East Java Drive

Sunnyvale, CA 94089

Telephone: +1 (408) 822-6000

Fax: +1 (408) 822-4501

Support Telephone: +1 (888) 4-NETAPP

Documentation Comments: mailto:info@netapp.com

Information Web: <http://www.netapp.com/>



# What NetApp Management Console is

---

NetApp Management Console is the client platform for NetApp Manageability Software applications. NetApp Management Console is used by administrators to carry out management tasks aided by DataFabric Manager, but it runs on a Windows or Linux system separate from the server on which DataFabric Manager is installed.

NetApp Management Console allows storage, application, and server administrators to perform management tasks such as data backup protection, space management, resource provisioning, data migration, and performance tuning, without having to switch between separate user interfaces.

The DataFabric Manager server provides infrastructure services (such as discovery, monitoring, role-based access control (RBAC), auditing, and logging for products in the storage and data suites) for NetApp Manageability Software client applications. The DataFabric Manager software runs on a separate server and is managed itself through Operations Manager, the Web-based user interface of DataFabric Manager. For more information about DataFabric Manager and Operations Manager, see the *Operations Manager Administration Guide*.

## Related information

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)



# Applications that run in NetApp Management Console

---

The Performance Advisor and the licensed Protection Manager and Provisioning Manager applications run in NetApp Management Console .

**Performance Advisor** This application provides a single location from which you can view comprehensive information about storage system and MultiStore vFiler unit performance and perform short-trend analysis. The application also helps you identify in the data infrastructure causes and potential causes of reduced performance.

Performance Advisor is automatically enabled with the Operations Manager Core license. For more information, see the *Performance Advisor Administration Guide* .

**Protection Manager** This application provides a policy-based management tool to help you unify and automate backup and mirroring operations. The application uses a holistic approach to data protection. It provides end-to-end, workflow-based design and seamless integration of SnapVault, SnapMirror, and Open Systems SnapVault to enable you to manage large-scale deployments easily.

The disaster recovery feature of the licensed protection application enhances your data protection services by enabling you to continue to provide data access to your users, even in the event of mishap or disaster that disables or destroys the storage systems in your primary data node. If disaster recovery protection is installed, you can quickly enable your secondary storage systems to provide primary data storage access to your users with little or no interruption, until your primary storage systems are reenabled or replaced.

To enable the protection features, you must purchase the protection license and install it on the DataFabric Manager server. The disaster recovery feature is a licensed option for Protection Manager.

**Provisioning Manager** This application helps you simplify and automate the tasks of provisioning and managing storage. The application provides policy-based provisioning and conformance of storage in datasets. The application also enables you to manually add volumes or qtrees to a dataset at any time, provides manual controls for space and capacity management of existing storage and newly provisioned storage, and allows you to migrate datasets offline to a new storage destination.

To enable the provisioning features, you must purchase the provisioning license and install it on the DataFabric Manager server.

**Related information**

*Performance Advisor Administration Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# NetApp Management Console window layout and navigation

---

You can navigate NetApp Management Console to move within and between applications, to display Help, and to log out of the console.

<b>Learning about Protection Manager</b>	The Get Started section of the user interface provides an overview of Protection Manager, a short tutorial that demonstrates how to set up protection, and a list of frequently asked questions (FAQs).
<b>Learning about disaster recovery</b>	The Get Started section of the user interface provides an overview of disaster recovery, a short tutorial that demonstrates how to set up disaster recovery, and a list of frequently asked questions (FAQs).
<b>Learning about Provisioning Manager</b>	The Get Started section of the user interface provides an overview of Provisioning Manager, a short tutorial that demonstrates how to set up provisioning, and a list of frequently asked questions (FAQs).
<b>Moving back and forth between panes</b>	The Back and Forward arrow buttons toggle between your last and previous panes, even if the pane was in a different application.
<b>Toggling between applications</b>	<ul style="list-style-type: none"> <li>• To use Protection Manager or Provisioning Manager, select <b>Tasks</b>  <b>&gt; Manage Data</b> or go to the Tasks Bar and click .</li> <li>• To use Performance Advisor, select <b>Tasks</b> <b>&gt; Manage Performance</b>  or go to the Tasks Bar and click .</li> </ul>
<b>Displaying help</b>	<ul style="list-style-type: none"> <li>• To display the Help for all applications on NetApp Management Console , click <b>Help</b> <b>&gt; Help Contents</b>.</li> <li>• To display Help for the specific window that is currently displayed, click <b>Help</b> <b>&gt; Help For This View</b> or click .</li> </ul>
<b>Logging out</b>	<ul style="list-style-type: none"> <li>• To log out, select <b>File</b> <b>&gt; Log Out</b> or click the logout button.</li> <li>• To log out and close NetApp Management Console , select <b>File</b> <b>&gt; Exit</b>.</li> </ul>
<b>Viewing product license information</b>	To view information about the product licenses you have installed, click <b>Help</b> <b>&gt; About</b> <b>&gt; Licenses</b> . Removed or added licenses are reflected in the license list after you restart NetApp Management Console .

Applications that run in NetApp Management Console vary in the specifics of their window layout. However, the windows are generally divided into two panes:

- Use the navigation pane on the left to move within an application.
- Use the content pane on the right to view and manage data. The content pane is generally divided into two areas: lists of selectable data and details of the selected data. Click  when it is displayed, for additional details.

**Note:** Specific applications might have additional navigation features not described in this section. In addition, software version incompatibility may result in some reduced functionality, which may cause some menu options or buttons to be disabled.

#### Related concepts

[Welcome to NetApp Management Console Help](#) on page 19

[NetApp Management Console window customization](#) on page 33

[NetApp Management Console data filtering](#) on page 35

# NetApp Management Console window customization

---

NetApp Management Console includes features you can use to customize the application window layout. By customizing application windows, you can control which data is viewable or how it is displayed.

**Note:** Not all customization features are available for every application window.

<b>Hiding or redisplaying the Tasks Bar</b>	You can hide the Tasks Bar to increase the space available for the content pane. (The overall width of the window remains the same when the bar is hidden.) You use the View menu to hide or display the bar.
<b>Selecting columns to display</b>	In content panes that include a list divided into columns, you can choose which columns you want to display. To display or hide a column, click the column-selection icon in the upper-right corner above the scroll bar (  ) , then click the name of a column heading from the selection list. Columns already displayed are identified with a check mark.  <b>Note:</b> The default version of a list does not necessarily include all available columns. You might find additional columns available in the column selection list.
<b>Readjusting column widths</b>	In content panes that include a list divided into columns, you can adjust the width of individual columns by horizontally dragging the vertical line between column headings. If accommodating all the columns you want to include results in column widths that obscure data, you can still see the entire value of a column field by putting your cursor over the field. A tool tip pops up, displaying the entire value of the field. You can maximize data visibility across all columns by clicking the column selection icon (  ) and choosing Pack All Columns.
<b>Rearranging column order</b>	In content panes that include a list divided into columns, you can rearrange the column order for a session by dragging and dropping column headings horizontally within the table. The arrangement persists until you exit the console.
<b>Reapportioning a content pane</b>	A splitter bar divides a content pane list area from the details area. You can move the splitter bar to increase or decrease the proportion of the content pane that displays the list of selectable data.

## Related concepts

[NetApp Management Console window layout and navigation](#) on page 31

*NetApp Management Console data filtering* on page 35

# NetApp Management Console data filtering

---

You can use the data filtering features to display only data meeting the criteria you specify.

In large-scale environments, the content pane might list so much data that it becomes difficult to locate the information you want. Filtering the data by specified criteria helps you focus on the issues most important to you.

**Note:** Not all filtering features are available for every application window.

**Filtering by group** The Group selection list in the toolbar enables you to display only the data that pertains to objects in a selected group. This setting persists until you log out or choose a different group.

**Filtering by regular expression** You can filter columns displaying site-specific values, such as storage system names or dataset names, by regular expression. To filter a column by regular expression, click the filter icon in the column heading (  ) and specify the regular expression to match against values in the column field. Headings of filtered columns are highlighted to remind you that some data is not currently displayed.

NetApp Management Console uses Java regular expression syntax for filtering data. For example:

- To view only items beginning with the letters "sch," type **sch** in the filter field, which matches Schedule but not SnapMirror.
- To view only items containing "space" somewhere in their string, type **.\*space** in the filter field, which matches strings such as Volume Space Normal.
- To view only items ending with the string "ok," type **\*ok** in the filter field, which matches strings such as SnapMirror: Date Ok.

**Filtering by column values** When a column displays a set of predefined possible values, you can choose to display only the rows of data that include a selected value. To filter a column by a specific, predefined value, click the filter icon in the column heading (  ) and select the predefined value from the drop-down list. Headings of filtered columns are highlighted to remind you that some data is not currently displayed.

**Filtering by column view** You can click  in the upper-right corner of the list to select which columns you want displayed.

**Sorting by column values** You can click on the column header to change the sort order of the column entries. When you click the column header, the sort arrow appears for that column.

## Related concepts

[\*NetApp Management Console window layout and navigation\*](#) on page 31

[\*NetApp Management Console window customization\*](#) on page 33

[\*What groups are\*](#) on page 1047

## Notifications

---

All applications installed on NetApp Management Console share the alarms and events functions.

Information in this Help about events and alarms applies to all applications installed on NetApp Management Console , except where application-specific information is specified.



# Descriptions of severity types

---

*Events* are generated automatically when a predefined condition occurs or when an object crosses a threshold. *Event messages* inform you when specific events occur. All events are assigned a severity type and are automatically logged in the **Events** window.

You can configure alarms to send notification automatically when specific events or severity types occur. If an application is not configured to trigger an alarm when an event is generated, you can find out about the event by checking the **Events** window.

It is important that you take immediate corrective action for events with severity level Error or worse. Ignoring such events can lead to poor performance and system unavailability.

**Note:** Event types are predetermined. Although you cannot add or delete event types, you can manage notification of events.

Each event is associated with a severity type to help you determine priorities for taking corrective action, as follows.

**Note:** Performance Advisor uses only the Normal and Error events.

Severity type	Description
Normal	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds. To view events with this severity type, you select the All option.
Information	The event is a normal occurrence. No action is required.
Warning	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption, and corrective action might not be required.
Error	The event source is still performing; however, corrective action is required to avoid service disruption.
Critical	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
Emergency	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
Unknown	The event source is in an unknown transitory state. To view events with this severity type, you select the All option.
Unmanaged	The event source is not managed by the protection or provisioning applications. No action is required.

**Related concepts**

*What alarms are* on page 71

**Related references**

*List of events and severity types* on page 43

# How to know when an event occurs

---

You can learn about event occurrences by viewing the event log or by configuring alarms to automatically notify you when events occur.

- Viewing the event log

You can use the **Events** window to view a list of all events that occurred and to view detailed information about any selected event.

- Configuring alarms

You can use the **Alarms** window to add an alarm that sends notifications automatically when an event occurs.

## Related tasks

[\*Monitoring events\*](#) on page 65

[\*Adding alarms\*](#) on page 601



# List of events and severity types

---

These tables list all of the events generated by Protection Manager, Provisioning Manager, and Operations Manager and the associated event severity types. Events are listed in alphabetical order by object type.

Use the links in the following table to jump directly to the events for that object.

**Note:** Performance Advisor uses only the Normal and Error events.

Event categories		
<a href="#">Active/Active Configuration Controller</a> on page 44 <a href="#">Active/Active Configuration Interconnect</a> on page 44 <a href="#">Active/Active Configuration Partner</a> on page 44 <a href="#">Agent</a> on page 45 <a href="#">Aggregate</a> on page 45 <a href="#">Alarm</a> on page 46 <a href="#">CFO Interconnect</a> on page 46 <a href="#">CFO Partner</a> on page 46 <a href="#">CFO Settings</a> on page 46 <a href="#">CFO This Storage System</a> on page 46 <a href="#">Configuration Changed</a> on page 47 <a href="#">CPU</a> on page 47 <a href="#">Data Protection</a> on page 47 <a href="#">Database</a> on page 47 <a href="#">Dataset</a> on page 48 <a href="#">Dataset Conformance</a> on page 49 <a href="#">Disks</a> on page 49 <a href="#">Enclosures</a> on page 49 <a href="#">Fans</a> on page 50	<a href="#">FC (Fibre Channel) Switch Port</a> on page 50 <a href="#">Filer Configuration</a> on page 50 <a href="#">Global Status</a> on page 50 <a href="#">HBA Port</a> on page 51 <a href="#">Host</a> on page 51 <a href="#">Host Agent</a> on page 52 <a href="#">Inodes</a> on page 52 <a href="#">Interface Status</a> on page 52 <a href="#">LUN</a> on page 52 <a href="#">Management Station</a> on page 53 <a href="#">Migration</a> on page 53 <a href="#">NDMP</a> on page 54 <a href="#">Network</a> on page 54 <a href="#">Network Services</a> on page 54 <a href="#">No Schedule Conflict</a> on page 55 <a href="#">NVRAM Battery</a> on page 55 <a href="#">OSSV (Open Systems SnapVault)</a> on page 55 <a href="#">Performance Advisor</a> on page 55 <a href="#">Power Supplies</a> on page 55 <a href="#">Primary</a> on page 56	<a href="#">Protection Policy</a> on page 56 <a href="#">Protection Schedule</a> on page 56 <a href="#">Provisioning Policy</a> on page 56 <a href="#">Qtree</a> on page 56 <a href="#">Remote Platform Management (RPM)</a> on page 57 <a href="#">Resource Group</a> on page 57 <a href="#">Resource Pool</a> on page 57 <a href="#">SAN Host LUN Mapping</a> on page 57 <a href="#">Script</a> on page 58 <a href="#">SnapMirror</a> on page 58 <a href="#">Snapshot(s)</a> on page 59 <a href="#">SnapVault</a> on page 60 <a href="#">SNMP Trap Listener</a> on page 60 <a href="#">Sync</a> on page 61 <a href="#">Temperature</a> on page 61 <a href="#">Unprotected Item</a> on page 61 <a href="#">User</a> on page 61 <a href="#">vFiler Unit</a> on page 62 <a href="#">vFiler Unit Template</a> on page 62 <a href="#">Volume</a> on page 62

### Active/Active Configuration Controller

Event name	Severity
Can Take Over	Normal
Cannot Takeover	Error
Dead	Critical
Takeover	Warning

### Active/Active Configuration Interconnect

Event name	Severity
Down	Error
Not Present	Warning
Partial Failure	Error
Up	Normal

### Active/Active Configuration Partner

Event name	Severity
Dead	Warning
May Be Down	Warning
OK	Normal

### Active/Active Configuration Settings

Event name	Severity
Disabled	Normal
Enabled	Normal
Not Configured	Normal
Takeover Disabled	Normal
This Controller Dead	Warning

**Agent**

Event name	Severity
Down	Error
Login Failed	Warning
Login OK	Normal
Up	Normal

**Aggregate**

Event name	Severity
Almost Full	Warning
Almost Overcommitted	Warning
Deleted	Information
Discovered	Information
Failed	Error
Full	Error
Nearly Over Deduplicated	Warning
Not Over Deduplicated	Normal
Not Overcommitted	Normal
Offline	Error
Online	Normal
Overcommitted	Error
Over Deduplicated	Error
Restricted	Normal
Snapshot Reserve Almost Full	Warning
Snapshot Reserve Full	Warning
Snapshot Reserve OK	Normal
Space Normal	Normal

## Alarm

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

## CFO Interconnect

Event name	Severity
Down	Error
Not Present	Warning
Partial Failure	Error
Up	Normal

## CFO Partner

Event name	Severity
Dead	Warning
May Be Down	Warning
OK	Normal

## CFO Settings

Event name	Severity
Disabled	Normal
Enabled	Normal
Not Configured	Normal
Takeover Disabled	Normal
This Node Dead	Warning

## CFO This Storage System

Event name	Severity
Can Take Over	Normal

Event name	Severity
Cannot Take Over	Error
Dead	Critical
Takeover	Warning

### Configuration Changed

Event name	Severity
Config Group	Information

### CPU

Event name	Severity
Load Normal	Normal
Too Busy	Warning

### Data Protection

Event name	Severity
Job Started	Information
Policy Created	Information
Policy Modified	Information
Schedule Created	Information
Schedule Modified	Information

### Database

Event name	Severity
Backup Failed	Error
Backup Succeeded	Information
Restore Failed	Error
Restore Succeeded	Information

## Dataset

Event name	Severity
Backup Aborted	Warning
Backup Completed	Normal
Backup Failed	Error
Created	Information
Deleted	Information
DR State Ready	Information
DR State Failover Over	Warning
DR State Failed Over	Information
DR State Failover Error	Error
DR Status Normal	Information
DR Status Warning	Warning
DR Status Error	Error
Initializing	Information
Job Failure	Warning
Member Clone Snapshot Discovered	Information
Member Clone Snapshot Status OK	Information
Member Dedupe Operation Failed	Error
Member Dedupe Operation Succeeded	Normal
Member Destroyed	Information
Member Destroy Operation Failed	Information
Member Resized	Information
Member Resize Operation Failed	Information
Modified	Information
Protected	Normal
Protection Failed	Error
Protection Lag Error	Error
Protection Lag Warning	Warning

Event name	Severity
Protection Suspended	Warning
Protection Uninitialized	Normal
Provisioning Failed	Error
Provisioning OK	Normal
Space Status: Normal	Normal
Space Status: Warning	Warning
Space Status: Error	Error
Write Guarantee Check - Member Resize Required	Warning
Write Guarantee Check - Member Size OK	Normal

## Dataset Conformance

Event name	Severity
Conformant	Normal
Conforming	Information
Initializing	Information
Nonconformant	Warning

## Disk

Event name	Severity
No Spares	Warning
None Failed	Normal
None Reconstructing	Normal
Some Failed	Error
Some Reconstructing	Warning
Spares Available	Normal

## Enclosures

Event name	Severity
Active	Information

Event name	Severity
Disappeared	Warning
Failed	Error
Found	Normal
Inactive	Warning
OK	Normal

### Fans

Event name	Severity
Many Failed	Error
Normal	Normal
One Failed	Error

### FC (Fibre Channel) Switch Port

Event name	Severity
Faulty	Error
Offline	Warning
Online	Normal

### Filer Configuration

Event name	Severity
Changed	Warning
OK	Normal
Push Error	Warning
Push OK	Normal

### Global Status

Event name	Severity
Critical	Critical
Non Critical	Error

Event name	Severity
Non Recoverable	Emergency
OK	Normal
Other	Warning
Unknown	Warning

### HBA Port

Event name	Severity
Offline	Warning
Online	Normal
Port Error	Error
Traffic High	Warning
Traffic OK	Normal

### Host

Event name	Severity
Cluster Configuration Error	Error
Cluster Configuration OK	Normal
Cold Start	Information
Deleted	Information
Discovered	Information
Down	Critical
Identity Conflict	Warning
Identity OK	Normal
Login Failed	Warning
Login OK	Normal
Modified	Information
Name Changed	Information
SNMP Not Responding	Warning

Event name	Severity
SNMP OK	Normal
System ID Changed	Information
Up	Normal

### Host Agent

Event name	Severity
Down	Error
Up	Normal
Host Agent: Login Failed	Warning

### Inodes

Event name	Severity
Almost Full	Warning
Full	Error
Utilization Normal	Normal

### Interface Status

Event name	Severity
Down	Error
Testing	Normal
Unknown	Normal
Up	Normal

### LUN

Event name	Severity
Offline	Warning
Online	Normal
Snapshot Not Possible	Warning
Snapshot Possible	Normal

## Management Station

Event name	Severity
Enough Free Space	Normal
File System File Size Limit Reached	Error
License Expired	Error
License Nearly Expired	Warning
License Not Expired	Normal
Load OK	Normal
Load Too High	Warning
Node Limit Nearly Reached	Warning
Node Limit OK	Normal
Node Limit Reached	Error
Not Enough Free Space	Error
Provisioning Manager Node Limit Nearly Reached	Warning
Provisioning Manager Node Limit Ok	Normal
Provisioning Manager Node Limit Reached	Error
Protection Manager Node Limit Nearly Reached	Warning
Protection Manager Node Limit Ok	Normal
Protection Manager Node Limit Reached	Error

## Migration

Event name	Severity
Dataset Not Migrating	Normal
Dataset Migrating	Normal
Dataset Migrated With Errors	Warning
Dataset Migrated	Normal
Dataset Migrate Failed	Error
vFiler Unit Not Migrating	Normal
vFiler Unit Migrating	Normal

Event name	Severity
vFiler Unit Migrated With Errors	Warning
vFiler Unit Migrated	Normal
vFiler Unit Migrate Failed	Error

## NDMP

Event name	Severity
Credentials Authentication Failed	Warning
Credentials Authentication Succeeded	Normal
Communication Initialization Failed	Warning
Communication Initialization Succeeded	Normal
Down	Warning
Up	Normal

## Network

Event name	Severity
OK	Normal
Too Large	Warning

## Network Services

Event name	Severity
CIFS Service - Up	Normal
CIFS Service - Down	Warning
NFS Service - Up	Normal
NFS Service - Down	Warning
iSCSI Service - Up	Normal
iSCSI Service - Down	Warning
FCP Service - Up	Normal
FCP Service - Down	Warning

## No Schedule Conflict

Event name	Severity
Between Snapshot and SnapMirror Schedules	Normal
Between Snapshot and SnapVault Schedules	Normal

## NVRAM Battery

Event name	Severity
Discharged	Error
Fully Charged	Normal
Low	Warning
Missing	Error
Normal	Normal
Old	Warning
Overcharged	Warning
Replace	Error
Unknown Status	Warning

## OSSV (Open Systems SnapVault)

Event name	Severity
Host Discovered	Information

## Performance Advisor

Event name	Severity
Enough Free Space	Normal
Not Enough Free Space	Error

## Power Supplies

Event name	Severity
Many Failed	Error
Normal	Normal

Event name	Severity
One Failed	Error

### **Primary**

Event name	Severity
Host Discovered	Information

### **Protection Policy**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

### **Protection Schedule**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

### **Provisioning Policy**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

### **Qtree**

Event name	Severity
Almost Full	Warning
Files Almost Full	Warning
Files Full	Error

Event name	Severity
Files Utilization Normal	Normal
Full	Error
Growth Rate Abnormal	Warning
Growth Rate OK	Information
Space Normal	Normal

### Remote Platform Management (RPM)

Event name	Severity
Online	Normal
Unavailable	Critical

### Resource Group

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

### Resource Pool

Event name	Severity
Created	Information
Deleted	Information
Modified	Information
Space Full	Error
Space Nearly Full	Warning
Space OK	Normal

### SAN Host LUN Mapping

Event name	Severity
Changed	Warning

## Script

Event name	Severity
Critical Event	Critical
Emergency Event	Emergency
Error Event	Error
Information Event	Information
Normal Event	Normal
Warning Event	Warning

## SnapMirror

Event name	Severity
Abort Completed	Normal
Abort Failed	Error
Break Completed	Normal
Break Failed	Error
Date OK	Normal
Delete Aborted	Warning
Delete Completed	Information
Delete Failed	Error
Initialize Aborted	Warning
Initialize Completed	Normal
Initialize Failed	Error
Nearly Out of Date	Warning
Not Scheduled	Normal
Not Working	Error
Off	Normal
Out of Date	Error
Possible Problem	Warning
Quiesce Aborted	Warning

Event name	Severity
Quiesce Completed	Normal
Quiesce Failed	Error
Resume Completed	Normal
Resume Failed	Error
Resync Aborted	Warning
Resync Completed	Normal
Resync Failed	Error
Unknown State	Warning
Update Aborted	Warning
Update Completed	Normal
Update Failed	Error
Working	Normal

## Snapshot(s)

Event name	Severity
Age Normal	Normal
Age Too Old	Warning
Count Normal	Normal
Count OK	Normal
Count Too Many	Error
Created	Normal
Failed	Error
Full	Warning
Schedule Conflicts with the SnapMirror Schedule	Warning
Schedule Conflicts with the SnapVault Schedule	Warning
Schedule Modified	Information
Scheduled Snapshots Disabled	Warning
Scheduled Snapshots Enabled	Normal

## SnapVault

Event name	Severity
Backup Aborted	Warning
Backup Completed	Information
Backup Failed	Error
Host Discovered	Information
Relationship Create Aborted	Warning
Relationship Create Completed	Information
Relationship Create Failed	Error
Relationship Delete Aborted	Warning
Relationship Delete Completed	Information
Relationship Delete Failed	Error
Relationship Discovered	Information
Relationship Modified	Information
Replica Date OK	Normal
Replica Nearly Out of Date	Warning
Replica Out of Date	Error
Restore Aborted	Warning
Restore Completed	Normal
Restore Failed	Error

## SNMP Trap Listener

Event name	Severity
Alert Trap Received	Information
Critical Trap Received	Information
Emergency Trap Received	Information
Error Trap Received	Information
Information Trap Received	Information
Notification Trap Received	Information

Event name	Severity
Warning Trap Received	Information
Start Failed	Warning
Start OK	Information

**Sync**

Event name	Severity
SnapMirror In Sync	Information
SnapMirror Out of Sync	Warning

**Temperature**

Event name	Severity
Hot	Critical
Normal	Normal

**Unprotected Item**

Event name	Severity
Discovered	Information

**User**

Event name	Severity
Disk Space Quota Almost Full	Warning
Disk Space Quota Full	Error
Disk Space Quota OK	Normal
Disk Space Soft Limit Exceeded	Warning
Disk Space Soft Limit Not Exceeded	Normal
E-mail Address OK	Normal
E-mail Address Rejected	Warning
Files Quota Almost Full	Warning
Files Quota Full	Error

Event name	Severity
Files Quota Utilization Normal	Normal
Files Soft Limit Exceeded	Warning
Files Soft Limit Not Exceeded	Normal

### vFiler Unit

Event name	Severity
Deleted	Information
Discovered	Information
Hosting Storage System Login Failed	Warning
IP Address Added	Information
IP Address Removed	Information
Renamed	Information
Storage Unit Added	Information
Storage Unit Removed	Information

### vFiler Unit Template

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

### Volume

Event name	Severity
Almost Full	Warning
Automatically Deleted	Information
Autosized	Information
Clone Deleted	Information
Clone Discovered	Information
Destroyed	Information

Event name	Severity
First Snapshot OK	Normal
Full	Error
Growth Rate Abnormal	Warning
Growth Rate OK	Normal
Maxdirsize Limit Nearly Reached	Information
Maxdirsize Limit Reached	Information
Nearly No Space for First Snapshot	Warning
Nearly Over Deduplicated	Warning
New Snapshot	Normal
Next Snapshot Not Possible	Warning
Next Snapshot Possible	Normal
No Space for First Snapshot	Warning
Not Over Deduplicated	Normal
Offline	Warning
Offline or Destroyed	Warning
Online	Normal
Over Deduplicated	Error
Quota Overcommitted	Error
Quota Almost Overcommitted	Warning
Restricted	Restricted
Snapshot Automatically Deleted	Information
Snapshot Deleted	Normal
Space Normal	Normal
Space Reserve Depleted	Error
Space Reservation Nearly Depleted	Error
Space Reservation OK	Normal

## Related concepts

[Descriptions of severity types](#) on page 39



# Monitoring events

---

You can view a list of all events that occurred and view detailed information about any event. You can also view deleted events that are marked for deletion.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed protection and provisioning applications, from the navigation pane, click **Notifications** ➤ **Events**. For Performance Advisor, from the navigation pane, click **Monitor** ➤ **Events**.
2. (Optional) You can customize the **Events** window in any of the following ways:
  - Select an event to view details about that event.
  - Click  in a column header to control which event entries you want displayed.
  - Click the sort arrows in a column header to change the sort order of the entries in that column.
  - Click  in the upper-right corner of the list to select which columns are displayed.
  - Drag the bottom of the events list area up or down to resize that area.
3. (Optional) You can view events that are marked for deletion by displaying hidden columns and removing a text filter, as follows:
  - a. Click  in the upper-right corner of the list and select the **Deleted By** and **Deleted Time** columns.
  - b. Click  in the Deleted By column header and delete the default search string.

The default filtering of deleted events is stopped and the deleted event entries are displayed in the list.

## Related concepts

[How to know when an event occurs](#) on page 41

## Related references

[Administrator roles and capabilities](#) on page 1055



# Responding to and acknowledging events

---

When an event occurs, you must take appropriate action to acknowledge and manage it and correct the problem. Responding to an event includes viewing it, acknowledging it, and correcting the problem.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Events**. For Performance Advisor, from the navigation pane, click **Monitor > Events**.
2. In the **Events** window, select an event to view the details about it.
3. Select an event and click **Acknowledge** to indicate that you are taking responsibility for managing that event.
4. In the Acknowledge Events dialog box, click **Yes** to acknowledge the selected event.

Your user name and the time are entered in the Events list for the selected event.

5. Find the cause of the event and take corrective action.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Deleting events

---

You can delete an event from the event list. Typically, you delete an event only after you acknowledge it and resolve the problem. However, you can also delete unacknowledged events if they are not important.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Events**. For Performance Advisor, from the navigation pane, click **Monitor > Events**.
2. In the **Events** window, select an event and click **Delete**.
3. In the Delete Events dialog box, click **Yes** to delete the selected event.
4. Verify that the event is deleted by viewing the **Events** window.

## After you finish

You can view events that are marked for deletion by clicking  in the corner of the list.

## Related references

[Administrator roles and capabilities](#) on page 1055



# What alarms are

---

Alarms are configured notifications that are sent whenever a specific event or an event of a specific severity type occurs, not necessarily related to a specific user. Alarms are used to monitor and manage datasets and resources.

Alarms are not the events themselves, only the notification of events. Alarms are not the same as user alerts. For a complete description of user alerts, see the *Operations Manager Administration Guide*.

You can create alarms for any defined resource group for which you want automatic notification of events. You use the **Alarms** window to add, monitor, and edit alarms.

## Related concepts

*Descriptions of severity types* on page 39

## Related information

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)



# Differences between alarms and user alerts

---

Configured event notifications provided by alarms are not the same as the automatic user-alert threshold messages sent to users.

You can configure alarms to notify specific recipients when specific events occur or when events of a specific severity type occur.

In contrast, alerts are notifications sent automatically to users who exceed space quotas. Whenever a user event related to disk or file quotas occurs, DataFabric Manager sends an alert to the user who caused the event. The alert is in the form of an e-mail message that includes information about the file system (volume or qtree) on which the user exceeded the threshold for a quota. You can disable the alerts either for all users or for the users who have quotas.

The following list summarizes the differences between alarms and user alerts.

**Configuring** Alarms: You must configure alarms before notification is sent to the specified recipients.

User alerts: User alerts are sent by default.

**Recipients** Alarms: Alarms can be sent to one or more of the following recipients:

- An e-mail address
- A pager e-mail address
- An SNMP trap host
- A script that you write

User alerts: User alerts are sent to the user who exceeds the user quota thresholds.  
User alerts can be only in the form of an e-mail message.

**Trigger** Alarms: You can configure alarms for any event, any event class, or any severity level.

User alerts: User alerts can be sent only when the following user quota events occur:

- User Disk Space Quota Almost Full
- User Disk Space Quota Full
- User Files Quota Almost Full
- User Files Quota Full



## Alarms triggered from related objects

---

When you create an alarm for a specific resource group, the alarm can be triggered by events that occur on resources that are related to the resource group, but that are not part of the resource group.

For example, if you create an alarm for a dataset that uses volumes, an alarm notification is also triggered when the storage system hosting one of the volumes goes down, even though the storage system itself is not a member of the resource pool for the dataset.

If one object is related to another object belonging to a resource group and is related closely enough to appear in the reports for that group, events on the related object might trigger alarms on that group.



# Guidelines for using alarms

---

You can optimize the use of alarms by following the guidelines listed below.

- Configure alarms for resource groups, not individual objects.

You can configure an alarm only for a defined group. If you want to create an alarm for a specific object, you must first create a group with that object as the only member and then create an alarm for that group.

- Select an appropriate event or severity level to trigger an alarm.

Not all events are severe enough to require alarms. Events that occur frequently might not be useful alarm candidates. Select only those events (or an event class) that are important enough to warrant special event notification.

- Make sure business-critical events are acknowledged.

Typically, alarms are set for business-critical events that must be acknowledged to establish a responsibility audit trail. Configure the Repeat Notify function to ensure that an event is acknowledged.

- Avoid multiple responses to the same event.

Not all alarms are important enough to require acknowledgment: for example, events of severity Normal or Information. By not configuring the Repeat Notify function, you avoid multiple responses to the same event.



# Alarm properties

---

You can configure or change the following properties when you add or edit an alarm. The properties are listed in the order in which they appear in the **Add Alarm** wizard.

- [\*Group\*](#) on page 82
- [\*Event Name or Severity\*](#) on page 82
- [\*Recipients\*](#) on page 82
- [\*Active Range\*](#) on page 82
- [\*Repeat Notify\*](#) on page 82
- [\*Enabled\*](#) on page 82

<b>Group</b>	The resource group the alarm is associated with. The default group is Global. You can associate an alarm with any resource group that is defined.
<b>Event Name or Severity</b>	Specifies what triggers the alarm: either when a specific event occurs, or when an event in an event class occurs, or when any event of a specified severity type occurs. If no specific event or severity type is selected when the alarm is added, the alarm applies to all events or severity types.
<b>By Event</b>	The event that triggers an alarm. When configuring an alarm, you can select a single event from the displayed list. For multiple events to trigger an alarm, you must first create an event class and then select that event class to trigger the alarm.
<b>By Severity</b>	The severity type that is the lowest severity level that triggers an alarm. All events that occur with the specified severity level trigger event notification. When configuring an alarm, you can select one of the following severity types: <ul style="list-style-type: none"><li>• Unknown The event is in an unknown state.</li><li>• Normal A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds.</li><li>• Information The event is a normal occurrence. No action is required.</li><li>• Unmanaged The event source is not managed by the protection or provisioning applications. No action is required.</li><li>• Warning</li></ul>

The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption, and corrective action might not be required.

- Error  
The event source is still performing; however, corrective action is required to avoid service disruption.
- Critical  
A problem occurred that might lead to service disruption if corrective action is not taken immediately.
- Emergency  
The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.

<b>Event Class</b>	The event class that triggers an alarm. When configuring an alarm, you can specify a previously defined event class; the occurrence of any event in the event class triggers the alarm. If you specify an event class, you can optionally specify a severity type; only the occurrence of an event in the event class with the specified severity type triggers the alarm. Use a regular expression to specify an event class: for example, env\temp.  You define event classes using Operations Manager. For information about event classes, see the <i>Operations Manager Administration Guide</i> .
--------------------	---

**Recipients** Specifies where the event notification is to be sent. Although all fields are optional, you must specify at least one recipient in one field.

<b>E-mail recipients</b>	<b>Administrator user names</b> One or more user names, separated by commas, of administrators who will receive the event notification by e-mail.
--------------------------	---

**Note:** Do not specify the e-mail address—that information is automatically obtained from the administrator profile information, which is configured using Operations Manager.

<b>Non-Administrators</b>	One or more e-mail addresses, separated by commas, of any other users who will receive the event notification by e-mail. Because there is no profile information available for non-administrators, you must specify the full e-mail address, in the following format: <i>name@domain.suffix</i> .
---------------------------	---

<b>Pager recipients</b>	<b>Administrator user names</b>	One or more user names, separated by commas, of administrators who will receive an event notification message at a pager e-mail address. Pager recipients receive shortened messages that are more suitable for small paging devices.
		<b>Note:</b> Do not specify the full pager e-mail address—that information is automatically obtained from the administrator profile information, which is configured using Operations Manager.
	<b>Non-Administrators</b>	One or more pager e-mail addresses, separated by commas, of any other user who will receive an event notification message at a pager e-mail address. Pager recipients receive shortened messages that are more suitable for small paging devices. Because there is no profile information available for non-administrators, you must specify the full pager e-mail address, in the following format: <i>name@domain.suffix</i> .
<b>Script</b>	<b>Script</b>	The full path name of a script that is executed when an alarm occurs. You can specify one script.
	<b>Run script as</b>	The user name to be used to run the script: for example, root.  This feature does not function in a Windows server environment. If a script is entered in this field, the script runs, but is ignored.
<b>SNMP trap hosts</b>	A comma-separated list of servers that contain an SNMP trap listener to receive the event notification. Use the following format: <i>community@host :portnumber</i> .	The default for <i>community</i> is <i>public</i> . For <i>host</i> , you can specify either an IP address or a name. For <i>portnumber</i> , you can specify a number in the range 1 through 65535. The default value is port 162.  For more information about SNMP traps, see the <i>Operations Manager Administration Guide</i> .

<b>Active range</b>	Specifies the time during which the alarm can be triggered. If a specific event or an event of a specified severity type occurs at a time at which the alarm is not active, no event notification occurs. For example, you might want an event notification to occur only when a specific administrator is available.
<b>Start</b>	Specifies the time at which the alarm becomes active, based on the time zone of the storage set to which the event notification applies.
<b>Stop</b>	Specifies the time at which the alarm becomes inactive, based on the time zone of the storage set to which the event notification applies.
<b>Repeat Notify (min)</b>	Specifies whether an alarm notification is repeated until the event is acknowledged and how often the notification is repeated. The default is no repeat notification.  <b>minutes value displayed</b> Repeats the event notification at the interval specified, until the event is acknowledged.  <b>no minutes value displayed</b> Event notification is sent only once and is not repeated.
<b>Enabled</b>	Specifies whether the alarm is currently enabled (selected) or disabled (not selected). The default is enabled.

#### Related concepts

[Decisions to make before adding an alarm](#) on page 83

#### Related tasks

[Adding alarms](#) on page 601

#### Related information

[Operations Manager Administration Guide -  
http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](#)

# Decisions to make before adding an alarm

---

Before you use the **Add Alarm** wizard to add a new alarm, you need to gather the information required to complete the wizard.

**Group** Which group will the alarm be associated with?

**Event or severity** What do you want to trigger the alarm?

- Decide if a specific event should trigger the alarm and, if so, which event.
- Decide if an event in an event class should trigger the alarm and, if so, which event class. And optionally, decide which severity type within the event class.
- Decide if any event of a specified severity type should trigger the alarm and, if so, which severity type.

**Recipients** Who or what needs to receive the event notification?

You can specify one or more of the following recipients:

- E-mails: Provide the administrator user names or non-administrator e-mail addresses.
- Pagers: Provide the administrator user names or non-administrator pager e-mail addresses.
- SNMP listener traps: Provide the host and port number of each SNMP trap. Optionally, provide the SNMP community name.
- Script: Provide the name of a script that is executed when an alarm occurs and the user name that runs the script.

**Active range** When should the event notification be active for the alarm?

**Repeat notification** Do you want the event notification repeated until the event is acknowledged? If so, how often do you want the notification to be repeated?

## Related tasks

[Adding alarms](#) on page 601

## Related references

[Alarm properties](#) on page 79



# Adding alarms

---

You can add an alarm when you want immediate notification that a specified event or event class or event of a specified severity level occurred.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available to complete this task:

- The resource group with which you want the alarm associated.
- The event name, event class, or severity type that triggers the alarm.
- Who and what you want the event notification sent to.
- The time period during which the alarm is active.
- Whether you want the event notification repeated until the event is acknowledged and how often the notification should be repeated.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click the **Set Up Alarms** window.
2. Click **Add** to start the **Add Alarm** wizard.
3. On each page of the wizard, enter the appropriate information.
4. Click **Finish** to commit your choices and close the **Add Alarm** wizard.
5. Verify the creation and configuration of the alarm by viewing the results that are displayed in the **Alarms** window.

## After you finish

You can edit the alarm properties from the **Alarms** window.

## Related concepts

[Decisions to make before adding an alarm](#) on page 83

[How to know when an event occurs](#) on page 41

## Related tasks

[How do I back up data?](#) on page 589

## Related references

[Alarm properties](#) on page 79

*Administrator roles and capabilities* on page 1055

# Testing alarms

---

You can test an alarm to check its configuration, after creating or editing the alarm.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click **Set Up > Alarms**.
2. Select an alarm and click **Test**.

You can select any alarm regardless of whether it is enabled or disabled.

3. Click **OK** in the Confirm Alarm(s) Test window to begin the test.

A test event notification is sent to each configured recipient. If a script is configured, the test notification runs the script.

4. Verify the alarm recipient configuration by checking that each recipient received a test message. If a script recipient is configured, check that the script was successfully started.

## After you finish

You can modify any of the alarm properties from the **Alarms** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Editing alarms

---

You can change the configuration of an existing alarm.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click **Set Up > Alarms**.
2. Select an alarm in the **Alarms** window and click **Edit**.
3. Use the tabs in the **Properties** sheet (Group, Event Type, Recipient, and Details) to change the configured property values.
4. Click **Apply** to commit your changes.
5. Click **OK** to close the **Properties** sheet.

The new configuration is immediately activated and displayed in the Alarms list.

6. Verify your changes by viewing the results that are displayed in the **Alarms** window.

Select an alarm to view the current property values for that alarm.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting alarms

---

You can delete an alarm when you no longer need immediate notification of an event or severity type.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click **Set Up > Alarms**.
2. Select one or more alarms in the **Alarms** window and click **Delete**.
3. Click **OK** in the Confirm Alarm(s) Delete dialog box to delete the selected alarms.

The alarm configurations are deleted and the alarms are removed from the Alarms list.

4. Verify your deletion by viewing the results that are displayed in the **Alarms** window.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Overview of alarm management tasks

---

Use the **Alarms** window to perform all alarm monitoring and managing tasks.

When responding to an alarm, you can use the **Events** window to view details about the event.

## Next topics

[Typical alarm management tasks](#) on page 93

[Infrequent alarm management tasks](#) on page 94

## Typical alarm management tasks

Alarm management tasks that you perform most often are responding to, viewing, editing, testing, and disabling or enabling alarms.

- Responding to alarms

When you receive an alarm, you should acknowledge the event and resolve the condition that triggered the alarm. If the repeat notification feature is enabled and the alarm condition persists, you continue to receive notifications until you acknowledge the event.

- Viewing the list of alarms

View the list of all currently configured data protection alarms when you want an overview of what is configured for any selected group. You can control the sort order of any column in the list. You can also control which alarms are displayed by filtering the information in any column in the list.

- Viewing the configuration values for any selected alarm

View the configuration details of any selected alarm when you want to know specific information or you are considering modifying the configuration.

- Editing an alarm

Modify the configuration of an alarm when you need to accommodate changes in the environment. For example, you might need to update a recipient e-mail address, add another recipient pager address, add a recipient script name, or change the hours during which the alarm is active.

- Testing an alarm

Test a new or modified alarm by having the licensed protection or provisioning application send a test message to all the recipients configured for the selected alarm.

- Disabling or enabling an alarm

Disable an alarm when you need to stop its functioning for awhile but want to retain the alarm configuration. For example, if you have an alarm configured for the SnapVault Backup Failed event and you scheduled down time for maintenance on that host, you might disable the alarm during the planned down time. When the host is up again, you can enable the alarm.

## Infrequent alarm management tasks

Alarm management tasks that you perform only occasionally are adding and deleting alarms.

- Adding an alarm

Configure a new alarm when you want notification of a specific event or any event of a specific severity type for a group.

- Deleting an alarm

Delete an alarm only when you are sure that you no longer need notification of the event or severity type occurring for the group.

# Responding to alarms

---

When you receive an alarm, you can acknowledge the event and resolve the condition that triggered the alarm.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

If the repeat notification feature is not enabled, you receive the event notification only once. If the repeat notification feature is enabled and the alarm condition persists, you continue to receive notifications until you acknowledge the event.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Events**. For Performance Advisor, from the navigation pane, click **Monitor > Events**.
2. Select an event whose details you want to view.
3. Click **Acknowledge** to indicate that you are taking responsibility for managing that event.
4. Click **Yes** in the Acknowledge Events dialog box to acknowledge the selected event.

Your user name and the time are entered in the Events list for the selected event.

5. Find the cause of the event and take corrective action.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Monitoring alarms

---

You can view a list of all the alarms configured for your application and the configuration values for each one.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click **Set Up > Alarms**.
2. (Optional) You can customize the **Alarms** window in any of the following ways:
  - Select an alarm to see the configured property values for that alarm.
  - Click  in a column header to control which alarm entries you want displayed. The color of the column header changes to indicate that you are filtering the entries in that column. Some column filters display a drop-down list to select from and other column filters display a search field in which you can enter text to select.
  - Click the sort arrows in a column header to change the sort order of the entries in that column.
  - Click  in the upper-right corner of the list to select which columns are displayed.
  - Drag the bottom of the alarms list area up or down to resize that area.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Enabling and disabling alarms

---

You can disable an alarm when you need to temporarily stop its functioning and enable it when you want it to start functioning again.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

Disabling an alarm enables you to retain the alarm configuration while its functioning is temporarily stopped. For example, if you have an alarm that is configured for the SnapVault Backup Failed event and you scheduled down time for maintenance on a host that is in the resource pool for the group associated with that alarm, you might disable the alarm during the planned down time. When the host is up again, you can enable the alarm to resume its functioning.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click **Set Up > Alarms**.
2. In the alarms list, locate the entry for the alarm you want to enable or disable.
3. Clear the **Enabled** check box to disable the associated alarm, or select the **Enabled** check box to enable it.

The alarm is immediately disabled or enabled.

4. Verify your change by viewing the results that are displayed in the **Alarms** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



## Role-based access control (RBAC)

---

Role-based access control (RBAC) provides the ability to control who has access to various client application features.

Applications use RBAC for user authorization. Administrators use RBAC to manage groups of users by defining roles. For example, if you need to control user access to resources, such as groups, datasets, and resource pools, you must set up administrator accounts for them. Additionally, if you want to restrict the information these administrators can view and the operations they can perform, you must apply roles to the administrator accounts you create.

**Note:** RBAC permission checks occur in the DataFabric Manager server. RBAC must be configured using the Operations Manager Web interface or command line interface.



# Administrator roles and capabilities

---

The administrator roles determine the tasks you can perform using applications in NetApp Management Console .

## Default and custom roles

One or more capabilities must be specified for every role, and you can assign multiple capabilities if you want the administrator to have more control than a specific role provides. For example, if you want an administrator to perform both the backup and restore operations, you must assign Back Up and Restore roles to the administrator.

The DataFabric Manager server and the client applications provide a set of default global roles described in the following list. You can customize these roles and the capabilities associated with them and you can create new ones using the Operations Manager Web-based user interface. For more information about configuring role-based access control (RBAC), see the *Operations Manager Administration Guide* .

<b>GlobalBackup</b>	You can initiate a backup to any secondary volume and ignore discovered hosts.
<b>GlobalDataProtection</b>	You can initiate a backup to any secondary volume; view backup configurations, events and alerts, and replication or failover policies; and import relationships into datasets.
<b>GlobalDataset</b>	You can create, modify, and delete datasets.
<b>GlobalDelete</b>	You can delete information in the DataFabric Manager server database, including groups and members of a group, monitored objects, custom views, primary and secondary storage systems, and backup relationships, schedules, and retention policies.
<b>GlobalEvent</b>	You can view, acknowledge, and delete events and alerts.
<b>GlobalFullControl</b>	You can view and perform any operation on any object in the DataFabric Manager server database and configure administrator accounts. You cannot apply this role to accounts with group access control.
<b>GlobalMirror</b>	You can create, destroy, and can update replication or failover policies.
<b>GlobalRead</b>	You can view the DataFabric Manager server database, backup and provisioning configurations, events and alerts, performance data, and policies.
<b>GlobalRestore</b>	You can restore the primary data back to a point in time or restore to a new location.
<b>GlobalWrite</b>	You can view or write to the DataFabric Manager server database.

<b>GlobalResourceControl</b>	You can add members to dataset nodes that are configured with provisioning policies.
<b>GlobalProvisioning</b>	You can provision primary dataset nodes and can attach resource pools to secondary or tertiary dataset nodes. The GlobalProvisioning role also includes all the capabilities of the GlobalResourceControl, GlobalRead, and GlobalDataset roles for dataset nodes that are configured with provisioning policies.
<b>GlobalPerfManagement</b>	You can manage views, event thresholds, and alarms apart from viewing performance information in Performance Advisor.

### Related concepts

[Strategies for enabling a dataset for migration](#) on page 779

### Related tasks

[Printing Help topics](#) on page 111

[Adding alarms](#) on page 601

[Testing alarms](#) on page 87

[Editing alarms](#) on page 89

[Deleting alarms](#) on page 91

[Responding to alarms](#) on page 95

[Monitoring alarms](#) on page 97

[Enabling and disabling alarms](#) on page 99

[Monitoring events](#) on page 65

[Responding to and acknowledging events](#) on page 67

[Deleting events](#) on page 69

[Adding a dataset](#) on page 719

[Assigning or changing a protection policy](#) on page 725

[Provisioning resources for a primary dataset node](#) on page 731

[Changing dataset node resource assignments](#) on page 739

[Adding resources to a dataset](#) on page 737

[Changing dataset node resource assignments](#) on page 739

[Removing resources from a dataset](#) on page 741

[Editing dataset general properties](#) on page 753

[Deleting a dataset](#) on page 755

[Adding a resource pool](#) on page 841

[Editing resource pool properties](#) on page 845

[Adding groups](#) on page 461

[Editing groups](#) on page 463

*Deleting groups* on page 465  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943  
*Updating Open Systems SnapVault client data* on page 945  
*Diagnosing a storage system* on page 947  
*Diagnosing an Open Systems SnapVault host* on page 949  
*Adding a daily protection schedule* on page 307  
*Adding a weekly protection schedule* on page 309  
*Adding a monthly protection schedule* on page 311  
*Adding a throttle schedule* on page 313  
*Deleting a protection or throttle schedule* on page 323  
*Assigning or changing schedules in a protection policy* on page 325  
*Copying a protection or throttle schedule* on page 327  
*Monitoring dataset status* on page 403  
*Monitoring backup and mirror relationships* on page 405  
*Backing up datasets on-demand* on page 407  
*Suspending protection of datasets* on page 409  
*Suspending data protection for backup volume maintenance* on page 411  
*Resuming protection of datasets* on page 413  
*Restoring backed-up data to a new location* on page 423  
*Restoring backed-up data over current data* on page 425  
*Restoring selected portions of a dataset* on page 427  
*Restoring a virtual machine to its original location* on page 429  
*Restoring a virtual machine file system to any location* on page 431  
*Restoring a virtual machine to its original location through another ESX server* on page 433  
*Importing discovered external relationships* on page 451  
*Adding unprotected host data to an existing dataset* on page 443  
*Adding unprotected host data to a new dataset* on page 445  
*Protecting unprotected datasets* on page 447  
*Starting a vFiler unit migration* on page 961  
*Updating vFiler unit migration SnapMirror relationships* on page 963  
*Cutting over to the new vFiler unit destination* on page 965  
*Cleaning up a vFiler unit migration* on page 967

- Cancelling a vFiler unit migration* on page 969
- Viewing vFiler unit migration status* on page 971
- Adding a protection policy* on page 671
- Editing a policy's primary data node* on page 258
- Editing a policy's backup connection* on page 259
- Editing a policy's backup node* on page 260
- Editing a policy's mirror connection* on page 260
- Editing a policy's mirror node* on page 261
- Changing retention times in a protection policy* on page 265
- Changing lag thresholds in a protection policy* on page 267
- Changing a node name in a policy* on page 269
- Deleting a protection policy* on page 271
- Editing a daily schedule* on page 315
- Editing a weekly schedule* on page 317
- Editing a monthly schedule* on page 319
- Editing a throttle schedule* on page 321
- Assigning or changing a provisioning policy* on page 727
- Configuring dataset nodes for NFS protocol access* on page 747
- Configuring dataset nodes for CIFS protocol access* on page 745
- Configuring dataset nodes for FC protocol access* on page 749
- Configuring dataset nodes for iSCSI protocol access* on page 751
- Displaying export properties for a specific dataset member* on page 417
- Displaying export and mapping information for all members of a dataset node* on page 415
- Monitoring failover readiness* on page 643
- Testing failover scripts* on page 644
- Updating disaster recovery node storage before failover* on page 646
- Starting failover* on page 647
- Monitoring failover status* on page 648
- Making the disaster recovery node the new primary data storage* on page 649
- Recovering by resuming forward mirroring* on page 651
- Recovering by resynchronizing data to undestroyed containers* on page 652
- Recovering by resynchronizing data to replaced containers* on page 654
- Testing failover scripts* on page 644
- Enabling disaster recovery protection* on page 641
- Adding a dataset* on page 719
  - Configuring dataset nodes for CIFS protocol access* on page 745
  - Configuring dataset nodes for NFS protocol access* on page 747
  - Configuring dataset nodes for iSCSI protocol access* on page 751
  - Configuring dataset nodes for FC protocol access* on page 749

*Assigning or changing a protection policy* on page 725  
*Provisioning resources for a primary dataset node* on page 731  
*Changing dataset node resource assignments* on page 739  
*Adding resources to a dataset* on page 737  
*Removing resources from a dataset* on page 741  
*Editing dataset general properties* on page 753  
*Deleting a dataset* on page 755  
*Viewing volume, LUN or qtree space allocation* on page 757  
*Diagnosing volume or qtree space status* on page 759  
*Diagnosing volume or qtree space status* on page 759  
*Resizing volume space* on page 761  
*Resizing qtree space* on page 763  
*Deleting Snapshot copies* on page 765  
*Deleting a volume, LUN or qtree* on page 767  
*Enabling deduplication on your dataset nodes* on page 809  
*Disabling deduplication on dataset nodes* on page 811  
*Starting on-demand deduplication* on page 813  
*Stopping an in-progress deduplication* on page 815  
*Viewing volume-level deduplication space-saving* on page 817  
*Adding a resource pool* on page 841  
*Editing resource pool properties* on page 845  
*Viewing a provisioning policy* on page 859  
*Adding a provisioning policy* on page 875  
*Editing a provisioning policy* on page 879  
*Copying a provisioning policy* on page 881  
*Deleting a provisioning policy* on page 883  
*Viewing vFiler templates* on page 889  
*Adding a vFiler template* on page 893  
*Editing a vFiler template* on page 895  
*Copying a vFiler template* on page 897  
*Deleting a vFiler template* on page 899  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943

- Updating Open Systems SnapVault client data* on page 945
- Diagnosing a storage system* on page 947
- Diagnosing an Open Systems SnapVault host* on page 949
- Monitoring jobs* on page 973
- Cancelling jobs* on page 975
- Starting a dataset migration* on page 783
- Updating dataset migration SnapMirror relationships* on page 785
- Cutting over to the new dataset storage destination* on page 787
- Cleaning up a dataset migration* on page 789
- Relinquishing migration capability of a dataset* on page 797
- Cancelling a dataset migration* on page 791
- Viewing dataset migration status* on page 793
- Assigning or changing a provisioning policy* on page 727

#### **Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Viewing NetApp Management Console configuration and licensing details

---

You can view information about NetApp Management Console , DataFabric Manager, the operating system, and other details from the Help menu.

## About this task

When troubleshooting issues with your system, it can be helpful to know about some of the system details, such as the software version, the operating system version, installation directory, memory availability, installed licenses, and so forth.

## Steps

1. In NetApp Management Console , from the Help menu, click **About**.

The About NetApp Management Console dialog box opens.

2. Select the information you want to view.

- a. Click **Configuration** to view details about software versions, installation directories, memory, and so forth.
- b. Click **Licenses** to view a list of the applications enabled in NetApp Management Console .

3. Click **OK** to close the dialog box.



# Printing Help topics

---

You can print one or more topics from the online Help.

## Before you begin

You must have the online Help displayed.

## Steps

1. In the online Help Table of Contents, select the topic or topics you want to print.

To print a single topic, select the topic.

To print multiple topics, use the **Shift** key to select multiple topics in a sequence. You can also use the **Ctrl** key to select multiple topics that are not in a sequence.

**Note:** Selecting a Table of Contents heading does not automatically select all the topics under that heading.

2. Click the print icon above the Help Table of Contents.

The print range in the Print dialog box indicates the number of print pages required for the selected topic or topics.

**Note:** For online Help, there is no distinction between the All and Pages options; both options print only the selected topic or topics.

## Related concepts

[Welcome to NetApp Management Console Help](#) on page 19

## Related references

[Administrator roles and capabilities](#) on page 1055



# Alarms window

---

You can use the **Alarms** window to monitor and configure alarms. You can also disable and enable alarms.

- [Command buttons](#) on page 563
- [Alarms list](#) on page 563
- [Details area](#) on page 564
- [Window customization](#) on page 565

## Command buttons

<b>Add</b>	Starts the <b>Add Alarm</b> wizard.
<b>Edit</b>	Opens the <b>Properties</b> sheet for modifying the configuration of the selected alarm.
<b>Delete</b>	Deletes the selected alarm.
<b>Test</b>	Tests the selected alarm by sending a test notification to all recipients.

## Alarms list

Displays a list of the currently configured alarms. The list is updated dynamically when the status changes.

<b>Event</b>	If the alarm is configured for a specific event, shows the event that triggers the alarm. Or, if the alarm is configured for an event class, shows the event class for which all events that occur in that class trigger the alarm.
<b>Severity</b>	If the alarm is configured for a severity type, shows the severity type that marks the lowest severity level that triggers the alarm. The default alarms list includes this column, which can be filtered to show a severity type and all severity types worse than the selected one.
<b>Unknown</b>	The event is in an unknown transitory state.
<b>Unmanaged</b>	The event source is not managed by the protection or provisioning applications. No action is required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds. No action is required.
<b>Information</b>	The event is a normal occurrence. No action is required.

<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Error</b>	The event source is still performing, but corrective action is required to avoid service disruption.
<b>Critical</b>	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
<b>Emergency</b>	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
<b>Group</b>	Shows the resource group the alarm is associated with. The default group is Global. You can associate an alarm with any resource group that is defined.
<b>Enabled</b>	Shows whether the alarm is currently enabled (selected) or disabled (not selected). The default is enabled.
<b>Details area</b>	
Displays detailed information about the selected alarm.	
<b>Event class</b>	Shows the class of events for which the alarm is configured. Event classes can only be selected; they are defined using Protection Manager, Provisioning Manager, or Operations Manager.
<b>Repeat Notify (min)</b>	Specifies whether an alarm notification is repeated until the event is acknowledged and how often the notification is repeated. The default is no repeat notification.
<b>minutes value displayed</b>	Repeats the event notification at the interval specified, until the event is acknowledged.
<b>no minutes value displayed</b>	Event notification is sent only once and is not repeated.
<b>Active range</b>	Specifies the time during which the alarm can be triggered. If a specific event or an event of a specified severity type occurs at a time at which the alarm is not active, no event notification occurs. For example, you might want an event notification to occur only when a specific administrator is available.
<b>Start</b>	Specifies the time at which the alarm becomes active, based on the time zone of the storage set to which the event notification applies.
<b>Stop</b>	Specifies the time at which the alarm becomes inactive, based on the time zone of the storage set to which the event notification applies.

**Recipients** Specifies where the event notification is to be sent.

**E-mails**

- |  |   |
|--|---|
| <b>Administrators</b><br><b>Non-Administrators</b> | Shows the administrators who will receive the event notification by e-mail.<br>Shows other users who will receive the event notification by e-mail. |
|--|---|

**Pagers**

- |  |   |
|--|---|
| <b>Administrators</b><br><b>Non-Administrators</b> | Shows the administrators who will receive an event notification message at a pager e-mail address.<br>Shows other users who will receive an event notification message at a pager e-mail address. |
|--|---|

**Traps**

- Shows the servers that contain an SNMP trap listener to receive the event notification.

**Script**

- |                                       |  |
|---------------------------------------|--|
| <b>Script</b><br><b>Run script as</b> | Shows the full path name of a script that is executed when an alarm occurs.<br>Shows the user name to be used to run the script. |
|---------------------------------------|--|

For more information about SNMP traps, see the *Operations Manager Administration Guide*.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

**Related information**

*Operations Manager Administration Guide -*

[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Events window

---

You can use the **Events** window to monitor, acknowledge, and delete events.

- [Command buttons](#) on page 559
- [View Events buttons](#) on page 559
- [Events list](#) on page 559
- [Details area](#) on page 561
- [Window customization](#) on page 561

## Command buttons

**Acknowledge** Acknowledges the selected events; your user name and the time are entered in the Event List for the selected events. When you acknowledge an event, you take responsibility for managing that event.

**Delete** Deletes the selected events from the Events summary list, so that the deleted events are not considered when calculating the status of a dataset, volume, and so forth. To view a list of deleted events, you can use the Operations Manager interface.

## View Events buttons

These filter buttons specify the range of events displayed in the events list.

- |                |  |
|----------------|--|
| <b>1 Day</b>   | Displays events that occurred today.   |
| <b>1 Week</b>  | Displays events that occurred in the last seven days.                              |
| <b>1 Month</b> | Displays events that occurred in the last 30 days.                                 |
| <b>All</b>     | Displays all events related to the NetApp Management Console client you are using. |

**Note:** On very large or very busy systems, the **Events** window might be unresponsive for long periods while loading **1 Month** or **All** data. If the application appears unresponsive for these large lists, select a shorter time period (such as **1 Day**).

## Events list

Displays a list of the events that occurred. The list of events is updated dynamically, as events occur. You can select an event to see the details for that event.

**Note:** The list of events that can be downloaded is limited to 25,000 records.

<b>Severity</b>	Displays the severity type. The default events list includes this column, which can be filtered to show a severity type and all severity types worse than the selected one.
The severity types are as follows.	
<b>Unknown</b>	The event is in an unknown transitory state.
<b>Unmanaged</b>	The event source is not managed by the protection or provisioning applications. No action is required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds. No action is required.
<b>Information</b>	The event is a normal occurrence. No action is required.
<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Error</b>	The event source is still performing, but corrective action is required to avoid service disruption.
<b>Critical</b>	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
<b>Emergency</b>	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
<b>Event</b>	Displays the event names. You can select an event to display the event details. The default events list includes this column.
<b>Triggered</b>	Displays the time and date the event was issued. The default events list includes this column.
<b>Acknowledged By</b>	Displays the user name of the person who acknowledged the event. The field is blank if the event is not acknowledged. The default events list includes this column.
<b>Acknowledged Time</b>	Displays the time the event was acknowledged. The field is blank if the event is not acknowledged. The default events list includes this column.
<b>Source</b>	Displays the full object name that triggered the event. The default events list includes this column.
<b>Deleted By</b>	Displays the user name that deleted the event. This column is not displayed by default.
<b>Deleted Time</b>	Displays the time the event was deleted. This column is not displayed by default.

## Details area

The area below the event list displays detailed information about the selected event, as follows:

<b>Event</b>	The event name.
<b>Source</b>	The full object name to which the event is associated.
<b>Source Type</b>	The object type that triggered the event.
<b>Severity</b>	The severity type of the event.
<b>About</b>	Additional description of the event.
<b>Triggered</b>	The time and date the event occurred.
<b>Acknowledged</b>	Whether the event was acknowledged and by whom.
<b>Deleted</b>	Whether the event was deleted from the Events list.
<b>Condition</b>	A description of the condition that triggered the event.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Overview of resource pools

---

A resource pool is a collection of unused physical storage resources, such as aggregates and disks, grouped together based on a user-defined set of common attributes.

You might pool your resources based on attributes such as performance, cost, physical location, or availability. By grouping related resources into a pool, you can treat the pool as a single unit for monitoring, provisioning, reporting, and role based access control (RBAC). This simplifies the management of these resources and allows for a more flexible and efficient use of the storage.

You create resource pools by using the **Add Resource Pool** wizard, which is accessible from the **Resource Pools** window. By using the wizard, you can select from a list of available aggregates, entire storage systems, or groups of physical resources from which to create your resource pool.

After you create a resource pool, you can associate it with one or more datasets. You can also associate datasets with provisioning and protection policies. These tasks can be accomplished when you add or edit datasets from the **Datasets** window.

When you assign a data protection policy, the licensed protection application applies the policy settings to automatically provision destination volumes from the assigned resource pool. It then creates backup and mirror relationships from each volume and qtree in the dataset to the newly provisioned secondary storage.

When you assign a provisioning policy to a dataset node, the licensed provisioning application applies the availability characteristics and space settings in the policy to automatically select the resources needed to fulfill a request for storage space for the primary data of a dataset.

These relationships between physical storage units, resource pools, and datasets mean that you must consider carefully what the impact might be of changes made to the system.

## Related concepts

[Dataset concepts](#) on page 693

[Decisions to make before adding datasets](#) on page 711

[Ways you might combine resources in resource pools](#) on page 825

[What groups are](#) on page 1047

[Decisions to make before assigning or changing policies](#) on page 721

**Related references**

*Advantages of using resource pools* on page 821

# Dataset concepts

---

You can use datasets to group data and use resource pools to group storage to simplify the monitoring, provisioning, reporting, and access control of your SnapVault and SnapMirror relationships, which enables flexible and efficient use of storage.

Associating a data protection, disaster recovery, or provisioning policy with a dataset lets storage administrators automate tasks, such as assigning consistent policies to primary data, propagating policy changes, and provisioning new volumes, qtrees, or LUNS on primary and secondary dataset nodes. The licenses that you have installed determine which policies are available.

Configuring a dataset combines the following objects:

<b>Dataset</b>	For protection purposes, a dataset is a collection of physical resources on a primary node, such as volumes, flexible volumes, and qtrees, and copies of backed-up data.  <b>Note:</b> It is a good practice to group primary data that have identical data protection requirements.
	For provisioning purposes, a dataset is a collection of physical resources, such as volumes, flexible volumes, qtrees, and LUNs, that are assigned to a dataset node. If the protection license is installed and the protection policy establishes a primary and one or more nonprimary nodes, each node of the dataset is a collection of physical resources that might or might not be provisioned from the same resource pool.
	A dataset cannot contain a storage system that is also in a resource pool assigned to a dataset node. This constraint prevents a loop that attempts to provision an infinite number of volumes.
<b>Application dataset</b>	A dataset managed by an application that is external to the licensed protection and provisioning applications, such as a dataset managed by SnapManager for Oracle.
<b>Resource pool</b>	A collection of physical resources from which secondary storage is provisioned. Resource pools can be used to group storage systems and aggregates by attributes, such as performance, cost, physical location, or availability.
<b>Data protection policy</b>	A data protection policy defines how to protect the primary, secondary, and tertiary storage, as well as when to create copies of data and how many copies to keep.
<b>Provisioning policy</b>	A provisioning policy defines how to provision primary or secondary dataset nodes, and provides rules for monitoring and managing storage space and for allocating storage space from available resource pools.

## Related concepts

[Overview of resource pools](#) on page 819

*What a policy is* on page 847

*What groups are* on page 1047

# What groups are

---

A *group* is a collection of objects with common characteristics, such as location, project, or owning organization.

The groups you create in the licensed protection and provisioning applications are the same as the resource groups you create in Operations Manager. You can create single-type groups of objects, or you can create groups that include combinations of object types. You can create groups of objects such as datasets, resource pools, storage systems, hosts, vFiler units, aggregates, volumes, and qtrees. Objects can be members of more than one group.

Combining objects in groups allows you to filter data for the objects in the group. Grouping datasets and resource pools also enables you to see consolidated reports of information in Operations Manager. See the Operations Manager online help for detailed descriptions of the default views for datasets and resource pools and the custom catalogs you can use to create your own reports.

**Note:** If necessary, you can use Operations Manager to specify Storage Resource Management or chargeback settings or to create groups containing other types of objects (LUNs, SRM paths, and so on).

## Related concepts

[NetApp Management Console data filtering](#) on page 35

[Overview of resource pools](#) on page 819

[Dataset concepts](#) on page 693

## Related tasks

[Changing dataset node resource assignments](#) on page 739



# About the NetApp Management Console dashboards

---

The dashboards provide a broad overview of various aspects of your data management environment.

If you are running more than one data management application, the specific dashboard panels that are displayed change according to the application that is currently selected.

**Protection dashboard** If you have the licensed protection application installed and you select the Protection dashboard, you can determine the current overall protection status of your systems,

such as the number of protected datasets versus unprotected datasets, system events to be addressed, and so forth. You can also gather data for evaluating system actions and to assist in determining how to set up datasets, resource pools, policies, and schedules for the future. If you installed and licensed the disaster recovery option, failover dashboard information is also displayed.

**Provisioning dashboard** If you have the licensed provisioning application installed and you select the Provisioning dashboard, you can determine the current overall status of dataset and resource pool provisioning. In addition to listing the top five events, information provided for datasets includes conformance status, resource status, and space status,

and information provided for resource pools includes space status and overall utilization. This information can help you determine when you need to increase available space for your datasets or when you need to investigate out-of-conformance issues.

**Performance dashboard** If you select **Monitor > Dashboard** in Performance Advisor, the default setting displays information about the current overall performance status of your systems,

such as top performance events, top storage systems by the total number of operations, top storage systems by network throughput, and storage systems by CPU utilization. If you have the proper permissions, you can modify the default settings to configure any view on the global group as a dashboard.

To access an application dashboard, you must have appropriate privileges. Items that you do not have privileges for are not displayed in the dashboard. If you encounter access problems, contact the administrator who maintains your DataFabric Manager roles and privileges.

You can filter the content of the Protection and Provisioning dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.

Information about the dashboard can be viewed by clicking the Help menu or . In the Protection and Provisioning dashboards, there is an additional Help icon available at the top of each dashboard panel that brings up a Help page with information about the panel.



# Dashboard panel descriptions

---

The dashboard panels provide cumulative at-a-glance status information for your system.

Dashboards are provided for each application available in NetApp Management Console .

- *[Protection dashboard](#)* on page 689 : These dashboard panels provide status on datasets, resource pools, protected data, and unprotected data.
- *[Provisioning dashboard](#)* on page 690 : These dashboard panels provide space management information related to datasets and resource pools.
- *[Performance Advisor dashboard](#)* on page 690 : These dashboard panels provide information on performance.

You can filter the content of some of the protection and provisioning dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools. When you select a group filter, only relationships originating or terminating at an object in the selected group are listed.

You must be assigned the appropriate privileges to view the dashboard panels.

## Protection dashboard

You can view more information about each dashboard panel and its contents by clicking  in the dashboard panel title bar to access the Help page for that panel.

<b>Failover Readiness</b>	Visible only when the disaster recovery option is licensed.  Displays the number of datasets configured for disaster recovery protection and that are in the failover ready state. This indicates that the datasets can successfully carry out failover operations, should failover operations become necessary.
<b>Failover Status</b>	Visible only when the disaster recovery option is licensed.  This panel appears when a failover operation is invoked, listing the number of datasets in the process of failing over and the number of datasets that have successfully failed over.
<b>Top Five Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events.
<b>Dataset Protection Status</b>	Displays the total number of protected datasets, grouped according to their current protection status value.
<b>Protected Data</b>	Displays the total number of datasets, volumes, qtrees, and Open Systems SnapVault directories that are covered by data protection policies.

<b>Unprotected Data</b>	Displays the total number of datasets, volumes, and qtrees that are not covered by data protection policies.
<b>Dataset Lags</b>	Displays any datasets that have a protection component that is out of date with the primary data. This panel groups relationships according to dataset, sorts relationships according to lag, selects the longest lag for each dataset, and displays the datasets in decreasing order of lag.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to and the space utilization for each resource pool. Items are sorted in increasing order of available space.

## Provisioning dashboard

You can view more information about each dashboard panel and its contents by clicking  in the task bar to access the Help page for that panel.

<b>Dataset Conformance Status</b>	Displays the total number of datasets that are conforming to associated policies.
<b>Top Five Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events.
<b>Dataset Resource Status</b>	Displays the number of datasets at different levels of resource status severity. The status represents the worst event severity on all direct and indirect members of the dataset nodes.
<b>Dataset Space Status</b>	Displays the total number of datasets being managed by NetApp Management Console , grouped according to their current space status value. The status represents the worst space status of all members in all nodes of the dataset. Events are generated at the dataset level when the space status of a dataset changes.
<b>Resource Pool Space Status</b>	Displays the total number of resource pools that currently meet or exceed the space thresholds.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to and the space utilization for each resource pool. Items are sorted in increasing order of available space.

## Performance Advisor dashboard

You can view more details about the Performance Advisor dashboard by clicking  in the task bar to access the dashboard Help page.

<b>Top Performance Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events. More detail about each event is provided in <b>Monitor &gt; Events</b> .
-------------------------------	--

<b>Top Storage Systems by Network Throughput</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest network throughput. The number above each bar chart displays the exact value of the throughput per second from that system. The vertical axis displays the megabytes of throughput per second. The horizontal axis displays the name of the storage system .
<b>Top Storage Systems by Total OPs</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest total operations. The vertical axis displays the total operations per second for that storage system . The horizontal axis displays the storage system name.
<b>Top Storage Systems by CPU Utilization</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest average CPU utilization. The number above each bar chart displays the exact value of the throughput per second from that system. The vertical axis displays the percentage CPU usage of the storage system . The horizontal axis displays the name of the storage system .



# How hosts become visible to the console

---

The hosts that you can view in NetApp Management Console and use in your policy implementations have been automatically discovered by DataFabric Manager or manually added to its database.

## Host discovery

When either Protection Manager or Provisioning Manager is enabled, DataFabric Manager automatically begins a host discovery process. The discovered hosts automatically display in the lists of storage system, vFiler unit, and Open Systems SnapVault client hosts in the provisioning and protection application interface.

When you add a host to NetApp Management Console, the host is incorporated into the DataFabric Manager database and is viewable in Operations Manager. You can add host systems in the management console from the **Storage Systems Hosts** window, **vFiler Units** window, and Open Systems SnapVault window.

Some items that are viewable as hosts in Operations Manager are not listed as hosts in the NetApp Management Console interface, because the console does not use items of that type to implement its data management tasks. For example, Fibre Channel switches are considered hosts in Operations Manager but are not included in the list of hosts in NetApp Management Console.

## Host monitoring

You can verify that a host is available and correctly configured by accessing the list in the appropriate Hosts window for storage systems, vFiler units, and Open Systems SnapVault systems. The protection and provisioning applications regularly check for updates to configuration information. This data is gathered from SNMP queries by system monitors. The monitors update the DataFabric Manager database at scheduled intervals. The protection and provisioning applications query the DataFabric Manager database for the information that is then displayed in NetApp Management Console.

Because the protection and provisioning applications do not query the hosts directly but rely on the scheduled monitors, the configuration information displayed in the Hosts windows is not real-time data. Therefore, this data might not reflect recent changes made to a storage system or configuration and could be outdated by a few minutes or a few hours, depending on the changes made.

For more information about host discovery and management with the DataFabric Manager database, see the *Operations Manager Administration Guide*.

## Related concepts

[Hosts that contain unprotected data](#) on page 439

## Related tasks

[How do I back up data?](#) on page 589

**Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## Ways to investigate problems with hosts

---

If you are investigating a policy failure, you can use the information displayed in the Hosts windows to determine whether the cause is a problem with a host. This information can also help determine the potential impact of any changes that you might make to a host.

Most problems that you might encounter with a host can be diagnosed and corrected by using the host diagnostics wizards. The diagnostics wizards are located on the **Storage Systems Hosts** window and the **OSSV Hosts** window. The wizards include steps to help you locate and fix issues with hosts. You can also use the Edit hosts property sheets to make changes to host licenses and host and NDMP credentials. You can access each of the wizards and property sheets in the following windows of the interface.

**Storage Systems Hosts window** Provides information about storage systems that can help you verify whether a host is up and accepting the NDMP credentials specified for it, as well as whether the appropriate licenses are assigned to it.

Allows you to review path and relationship information about storage systems, as well as to check host and NDMP status. The path and relationship information displayed for each individually selected storage system helps you see the interdependencies between hosts. For example, by reviewing the data flowing into and out of a selected storage system, you can evaluate the impact of temporarily removing that storage system from service for maintenance. You can also review information about input and output relationships to determine whether lag times are within specified thresholds and which datasets are impacted if the lag threshold has been or is about to be exceeded.

From this window, you can start the **Add Storage System** wizard and the **Diagnose Storage Systems** wizard, or you can open the Edit property sheet for storage systems. You can also refresh the information about a selected host in the window's host list.

**vFiler Units window** Allows you to review the status of vFiler units and to verify the IP address of the vFiler unit and the name of the storage system that is hosting it.

Allows you to review path and relationship information about vFiler units. The path and relationship information displayed for each individually selected vFiler unit helps you see the interdependencies between hosts and datasets. For example, by reviewing the data flowing into and out of a selected host, you can evaluate the impact of temporarily removing that host from service for maintenance.

From this window, you can start the Add vFiler Unit wizard or the Setup vFiler Unit wizard, and you can delete vFiler units.

<b>OSSV Hosts window</b>	<p>Allows you to review the status of Open Systems SnapVault hosts (including VMware ESX hosts) the port and credentials status of each NetApp Host Agent , and the status of NDMP connections and credentials.</p>
	<p>Allows you to investigate problems with an Open Systems SnapVault client. Information in this window includes the host and NDMP status, the NDMP credentials status, the operating system and version that each host is running, and path information for each host.</p>

From this window, you can start the **Add OSSV Host** wizard and the **Diagnose OSSV Host** wizard, and open the Edit OSSV host property sheet for a host that contains an Open Systems SnapVault agent.

From this window, you can also stop and start an Open Systems SnapVault 2.3 and later agent on which NetApp Host Agent is installed. Stopping and starting the agent stops and starts backup service on the selected client, which might resolve the problem. After you restart the backup service, you can click **Refresh** to display current data for the selected client and determine the effect of restarting the backup service.

**Note:** There is no Open Systems SnapVault plugin for Solaris, so the NetApp Host Agent cannot talk to the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the NetApp Management Console .

## Related tasks

[Diagnosing a storage system](#) on page 947

[Diagnosing an Open Systems SnapVault host](#) on page 949

# Data ONTAP licenses used for protecting or provisioning data

---

There are several Data ONTAP licensed options that you can use to protect or provision your data. After you have purchased the software licenses you need, you can assign these licenses to your primary and secondary storage from the **Storage Systems Hosts** window.

When you purchase a Data ONTAP option license, you receive a code composed of a string of characters, such as ABCDEFG, that is unique to a particular service. You receive license codes for every protocol and option, or service, that you purchase.

Not all purchased license codes are installed on a storage system before it is shipped from the factory. Some licenses are installed after the system is set up. You can purchase license codes to enable additional services at any time. If you misplace a license code, you can contact NetApp technical support or log in to the NOW site to obtain a copy.

You must enter a software license code on a storage system to enable the corresponding service. You do not need to indicate which license the code enables. The code is matched automatically to the appropriate service license.

**Note:** The Licenses area is visible only when the selected host is a single storage system running Data ONTAP. If you plan to use Open Systems SnapVault to back up data on a host that is not running Data ONTAP, you select the secondary storage system to license the necessary Data ONTAP services.

The licenses available for use with Data Manager are:

**SnapMirror license** You install a SnapMirror license on each of the source and destination storage systems for the mirrored data. If the source and destination volumes are on the same system, only one license is required.

SnapMirror replicates data to one or more networked storage systems. SnapMirror updates the mirrored data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on nonproduction systems, online data migration, and so on. You can also enable the SnapMirror license to use Qtree SnapMirror for backup.

To use SnapMirror software, you must update the `snapmirror.access` option in Data ONTAP to specify the destination systems that are allowed to access the primary data source system. For more information about the `snapmirror.access` option, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

**SnapVaultData ONTAP secondary license** You install the SnapVault Secondary license on storage systems hosting the backups of protected data. SnapVault creates backups of data stored on multiple primary storage systems and copies the backups to a secondary storage system. If data loss or corruption occurs, backed-up data can be restored to a primary

	<p>or open storage system with little of the downtime and uncertainty associated with conventional tape backup and restore operations.</p>
<b>SnapVaultData ONTAP primary license</b>	<p>You install the SnapVaultData ONTAP Primary license on storage systems running Data ONTAP that contain host data to be backed up.</p>
<b>SnapVault Windows Primary License</b>	<p>You install the SnapVault Windows Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a Windows-based primary storage system running the Open Systems SnapVault agent. A Windows-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>SnapVault Windows Open File Manager license</b>	<p>You install the SnapVault Open File Manager license on a secondary storage system to enable the backup of open files on Windows primary storage systems running the Open Systems SnapVault agent.</p> <p>You must install the SnapVault Windows Primary license and the SnapVaultData ONTAP Secondary license on the secondary storage system before installing the SnapVault Open File Manager license.</p>
<b>SnapVault UNIX primary license</b>	<p>You install the SnapVault UNIX Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a UNIX-based primary storage system (AIX, HP-UX, or Solaris) running the Open Systems SnapVault agent. A UNIX-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>SnapVault Linux primary license</b>	<p>You install the SnapVault Linux Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a Linux-based primary storage system running the Open Systems SnapVault agent. A Linux-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>NearStore Option license</b>	<p>The NearStore license enables your storage system to use transfer resources as conservatively as if it were optimized as a backup system. This approach is useful when the storage system on which you want to store backed-up data is not a system optimized for storing backups, and you want to minimize the number of transfer resources the storage system requires.</p> <p>Storage systems using the NearStore license must meet the following criteria:</p> <ul style="list-style-type: none"><li>• The storage system must be a FAS30xx , FAS31xx series , or FAS60xx system.</li><li>• The version of Data ONTAP software must be 7.1 or later.</li><li>• If you plan to use the SnapVault service, the storage system must have a SnapVault secondary license enabled.</li></ul>

<b>Deduplication license</b>	The deduplication license enables you to consolidate blocks of duplicate data into single blocks to store more information using less storage space.
<b>SnapMirror Sync license</b>	The SnapMirror Sync license enables you to replicate data to the destination as soon as it is written to the source volume. SnapMirror Sync is a feature of SnapMirror.
<b>MultiStore Option license</b>	<p>The MultiStore Option license enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems on the network. Each virtual "storage system" created as a result of the partitioning is called a vFiler unit. A vFiler unit, using the resources assigned, delivers file services to its clients as a storage system does.</p> <p>The storage resource assigned to a vFiler unit can be one or more qtrees or volumes. The storage system on which you create vFiler units is called the hosting storage system. The storage and network resources used by the vFiler units exist on the hosting storage system.</p> <p>Be sure the host on which you intend to install the MultiStore Option license is running Data ONTAP version 6.5 or later.</p>

## Related concepts

[When qtree SnapMirror is used to perform backups](#) on page 909

## Related tasks

[Adding a resource pool](#) on page 841

## Related information

[Data ONTAP Data Protection Tape Backup and Recovery Guide -](#)  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)



# **When qtree SnapMirror is used to perform backups**

The licensed protection application can use either SnapVault or qtree SnapMirror to perform backups. The protection application determines which technology to use based on the licenses enabled on the source and destination hosts and the schedule applied to the backup connection of the protection policy.

If you use only SnapVault licenses in your environment, the protection application uses SnapVault for backups. However, if you use both SnapVault and SnapMirror licenses in your environment, the protection application uses the following sequence to determine whether to use SnapVault or qtree SnapMirror for backups:

1. If the data to be backed up is located on a host running the Open Systems SnapVault agent, the protection application uses SnapVault for backups.
2. If either the source or destination host has the SnapMirror license enabled but not the SnapVault license, the protection application uses qtree SnapMirror for backups.
3. If both the source and destination host have the SnapVault license enabled but not the SnapMirror license, the protection application uses SnapVault for backups.
4. If the schedule applied to the backup connection specifies that the data needs to be backed up more frequently than once an hour, the protection application uses qtree SnapMirror for backups.
5. If none of the previous conditions applies, by default, the protection application uses SnapVault for backups.

## **Related references**

*[Data ONTAP licenses used for protecting or provisioning data](#)* on page 905



## How to customize a vFiler unit configuration using a script

---

You can write a script to customize a vFiler unit configuration. When the script is specified in the **Setup vFiler Unit** wizard, the licensed provisioning application executes the script before and after a vFiler unit is set up. You must specify the full DataFabric Manager server path of the script.

For example, if you want the new vFiler unit to use a vFiler unit configuration that was saved in Operations Manager, you might write a script that runs the appropriate `dfm config` commands to retrieve and execute that configuration.

For information on the environment variables you may need for a script, see the `dfpm` man pages in Operations Manager.



# Decisions to make before adding a storage system

Before running the **Add Storage System** wizard, it is useful to have all of the configuration information available for the host that you are adding.

**Host Name or IP Address** What is the name or the IP address of the storage system that you want to add?

**Licenses** Which services do you want enabled on the storage system?

You must enter a software license code to enable each corresponding service on the storage or host. Licenses are set immediately upon entering the information in the text field. License information cannot be removed or cancelled once entered, so be sure you are entering the correct storage system.

When you enable licenses, consider how you want to use each storage system to protect data:

- Can it be used to hold primary data or secondary data or both?
- Can it be used for backups or for mirroring?
- What operating system can it run on?

**Login Credentials** What are the user name and password for the storage system?

**Access Control** What roles do you want to have access privileges to the storage system?

You can assign different access privileges for SnapVault and for SnapMirror.

**NDMP Credentials** What is the NDMP user name for the storage system that you want to add?

DataFabric Manager automatically manages the password based on the user name provided. DataFabric Manager uses these credentials to communicate with the selected host over NDMP.

To obtain an encrypted NDMP password for a storage system, issue `ndmpd password username` from the command line of the storage system.

For more information about how Operations Manager uses NDMP, see the *Data ONTAP Storage Management Guide*. For more information about NDMP credentials, see the *Data ONTAP Data Protection Tape Backup and Recovery Guide*.

## Related tasks

[Adding a storage system](#) on page 915

**Related information**

*Data ONTAP Storage Management Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

*Data ONTAP Data Protection Tape Backup and Recovery Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

# Adding a storage system

---

You can add storage systems to the hosts list to make them available for inclusion in data management actions. When you add storage systems to NetApp Management Console, you also add the storage to the DataFabric Manager database.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available for the storage system that you want to add:

- Host name or IP address
- Host credentials (user name and password)
- License code
- SnapVault Access Control List, if licensed for SnapVault
- SnapMirror Access Control List, if licensed for SnapMirror
- NDMP credentials (user name and password)

## Steps

1. From the navigation pane, click **Hosts ▶ Storage Systems**.
2. Click **Add** to start the **Add Storage System** wizard.

Enter or select information as requested in the wizard.

**Note:** In this wizard, clicking Next implements the operations on each page. Clicking Back or Cancel does not undo operations performed on previous pages.

3. Verify that the storage system that you added is included in the hosts list in the **Storage Systems Hosts** window.

You might need to update the window before you can view the new host in the host list.

You can now manage data located on the new storage system or use the storage as a secondary storage system for backups or mirror copies.

## Related concepts

[Decisions to make before adding a storage system](#) on page 913

**Related tasks**

*[How do I back up data?](#)* on page 589

**Related references**

*[Administrator roles and capabilities](#)* on page 1055

# Decisions to make before adding an Open Systems SnapVault host

---

Before adding an Open Systems SnapVault host using the **Add OSSV Host** wizard, it is useful to have all of the host's configuration information available.

If the Open Systems SnapVault host you are adding resides on a VMwareESX 3.5 server, you should review the guidelines for adding an Open Systems SnapVault host on an ESX 3.5server.

**Host Name or IP Address** What is the name or the IP address of the Open Systems SnapVault host that you want to add?

**Host Agent Credentials**

- What are the user name and password that DataFabric Manager should use to authenticate to the host running NetApp Host Agent ?  
Operating system credentials for the host on which NetApp Host Agent is running, if DataFabric Manager is managing the credentials for you  
Credentials for NetApp Host Agent , if DataFabric Manager is NOT managing the credentials
- Should DataFabric Manager set up and manage the host agent password or will you do it manually?  
For instructions describing how to set up credentials for hosts running NetApp Host Agent , see the *NetApp Host Agent Installation and Administration Guide* .

**NetApp Host Agent Port** What port number do you want to use for host agent access?  
The default port is 4092.

**NDMP Credentials** What are the NDMP user name, password, and port number for the host that you want to add?  
DataFabric Manager uses these credentials to communicate with the selected host over NDMP.

To obtain an encrypted NDMP password for the host, issue `ndmpd password username` from the command line.

The default port number is 10000.

If the host runs the Open Systems SnapVault agent, specify the port number, if other than the default, that DataFabric Manager should use when communicating with the selected host over NDMP.

For more information about how Operations Manager uses NDMP, see the *Data ONTAP Storage Management Guide* . For more information about NDMP

credentials, see the *Data ONTAP Data Protection Tape Backup and Recovery Guide*.

For more information about Open Systems SnapVault configurations, see the *Open Systems SnapVault Installation and Administration Guide*.

#### **Related tasks**

[Adding an Open Systems SnapVault host](#) on page 921

#### **Related references**

[Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#) on page 919

#### **Related information**

*Open Systems SnapVault Installation and Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/client\\_filer\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/client_filer_index.shtml)

*Data ONTAP Storage Management Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

*Data ONTAP Data Protection Tape Backup and Recovery Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

# Guidelines for adding and editing an Open Systems SnapVault host on an ESX server

---

NetApp Management Console supports Open Systems SnapVault backups for virtual machines (VMs) on VMware ESX servers. Before starting the **Add OSSV Host** wizard for VMware® ESX 3.5, it is useful to review the following guidelines.

- The Open Systems SnapVault software must be installed on each VMware® ESX 3.5 server that you want to back up.
- The NetApp Host Agent is NOT needed for an Open Systems SnapVault installation on a VMware® ESX 3.5 server.
- DataFabric Manager discovers only the virtual machines that are registered to the VMware® ESX 3.5 server that you have discovered.
- NetApp Management Console backs up only the virtual machines on an VMware® ESX 3.5 server. File system backups on a VMware® ESX 3.5 server are not supported.
- The backup for the virtual machine is always through the VMware® ESX 3.5 server that was involved in creating the relationship.

If the virtual machine is moved to another server, the backup is still through the original VMware® ESX 3.5 server. If the original VMware® ESX 3.5 server is offline, the virtual machine is not backed up.

For more information about Open Systems SnapVault configurations, see the *Open Systems SnapVault Installation and Administration Guide*.

## Related concepts

[Decisions to make before adding an Open Systems SnapVault host](#) on page 917

## Related tasks

[Adding an Open Systems SnapVault host](#) on page 921

[Editing Open Systems SnapVault properties](#) on page 939

[How do I back up data?](#) on page 589

## Related information

[Open Systems SnapVault Installation and Administration Guide](#) -

[http://now.netapp.com/NOW/knowledge/docs/client\\_filer\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/client_filer_index.shtml)



# Adding an Open Systems SnapVault host

---

You can add an Open Systems SnapVault host to make the host available to Data Manager for inclusion in data management actions. When you add an Open Systems SnapVault host to Data Manager, you also add the host to the DataFabric Manager database.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If the Open Systems SnapVault host you are adding resides on a VMware® ESX 3.5 server, review the guidelines for adding an Open Systems SnapVault host on a VMware® ESX 3.5 server.

Have the following information available for the host that you want to add:

- Host name or IP address
- Port number for NetApp Host Agent
- Decision about whether DataFabric Manager should set up and manage the NetApp Host Agent password:
  - If yes, provide the operating system credentials for the host on which NetApp Host Agent is running.
  - If no, provide the credentials for NetApp Host Agent .
- NDMP credentials (user name and password) and port number

## Steps

1. From the navigation pane, click **Hosts > OSSV** .
2. Click **Add** to start the **Add OSSV Host** wizard. Enter or select information as requested in the wizard.
3. Verify that the host you added is included in the hosts list in the **OSSV Hosts** window.

You might need to refresh the window before you can view the new host in the host list.

## Related concepts

[Decisions to make before adding an Open Systems SnapVault host](#) on page 917

## Related tasks

[How do I back up data?](#) on page 589

### Related references

- [Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#)* on page 919
- [Administrator roles and capabilities](#)* on page 1055

## Decisions to make before adding a vFiler unit

---

Before starting the **Add vFiler Unit** wizard, it is useful to have all of the following configuration information available for the unit that are you adding.

<b>Name</b>	What is the name of the vFiler unit that you want to add?  The vFiler unit name must be unique to that vFiler unit.
<b>IP space</b>	What is the IP space for the vFiler unit that you want to add?  An IP space defines an address in which the vFiler unit can participate. If no IP space is defined for the vFiler unit, use default-ipspace. For more information about vFiler IP space, see the <i>Data ONTAP MultiStore Management Guide</i> .
<b>Allowed protocols</b>	What protocols are assigned to the vFiler unit?  The following protocols are supported: <ul style="list-style-type: none"><li>• iSCSI</li><li>• NFS</li><li>• CIFS</li></ul> Fibre Channel is not supported on vFiler units.  <b>Attention:</b> If you assign the CIFS protocol to the vFiler unit, you need to set up CIFS before you can use the vFiler unit. Performing the setup stops and restarts CIFS, interrupting the CIFS service.
<b>Parent storage system or resource pool</b>	What storage system or resource pool is the vFiler unit assigned to?  Be sure the host on which you want to create a vFiler unit is running Data ONTAP version 7.0 or later.
<b>IP address</b>	What is the IP address of the vFiler unit that you want to add?  The IP address used by the vFiler unit must not be configured for use before you create the vFiler unit.  <b>Note:</b> The IP address accepts both IPv4 and IPv6 address formats.
<b>Network mask</b>	What is the network mask of the vFiler unit that you want to add?  The Network mask is not required to create the vFiler unit, although you must specify a network mask in order to setup the vFiler unit.

**Network interface** What is the Ethernet interface for the vFiler unit?

The Ethernet interface is not required to create the vFiler unit, although you must specify an interface before you can use the vFiler unit. If you plan to run scripts on the vFiler unit, you might choose to wait to specify the Ethernet interface later, by using the Setup option.

**VLAN ID** Will you use VLANs in the creation of the vFiler unit? What is the ID of the VLAN that you will use?

VLANs allow you to partition a physical network into multiple virtual networks that are totally separate from one another.

If the vFiler unit that you plan to add is created on an active/active host, you can use an existing VLAN ID or create a new VLAN ID for the vFiler unit. If a VLAN ID is not entered, the Partner interface field is disabled.

**Partner interface** What is the partner interface for the vFiler unit?

If you create a vFiler unit using an active/active host, the partner interface is selected automatically. If no partner interface is configured, then the option None is selected automatically.

The storage system on which the vFiler unit is created needs to be configured as an active/active configuration before the creation of the vFiler unit.

**vFiler template** Which, if any, vFiler template do you want to use for the vFiler unit?

A vFiler template is a set of vFiler configuration settings and the corresponding CIFS configuration settings. If you do not select a vFiler template, the network settings are cleared.

**CIFS workgroup name** What is the Windows workgroup name for the CIFS setup?

The Windows workgroup name specifies the name of the shared resources. The workgroup name option is displayed if the following apply:

- You select to use the CIFS protocol
- You select the Perform CIFS setup option
- You do not select a vFiler template or the template you select does not include CIFS settings

If you set up the vFiler unit to use the CIFS protocol, the vFiler units can use the same computer names as the servers. This enables CIFS clients to share resources without having to remap their drives or search for the new server.

<b>CIFS domain user and domain password</b>	What is the login name and the password for administrative access to the Active Directory system?  The domain user and domain password options are displayed if the following apply:
	<ul style="list-style-type: none"><li>• You select to use the CIFS protocol</li><li>• You select the Perform CIFS setup option</li><li>• You select a vFiler template that specifies Active Directory for CIFS authentication</li></ul>
<b>Root password</b>	What password will you use for the vFiler unit you are creating?
<b>Script path</b>	Do you want to use a custom script to help manage vFiler units? If so, what is the full path of the script?  You can use the script while creating or setting up the vFiler unit.  <b>Note:</b> If the DataFabric Manager server is running on Windows, and if the post-setup script for the vFiler unit is on a network share, the script location must be specified by the full UNC path (no drive letter mapping).

### Related concepts

[What vFiler templates are](#) on page 885

[Considerations for active/active hosts](#) on page 933

### Related tasks

[Adding a vFiler unit](#) on page 927

### Related information

*Data ONTAP MultiStore Management Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)



# Adding a vFiler unit

---

You can create and configure vFiler units to make them available for inclusion in data management actions.

## Before you begin

Ensure that the host on which you want to create a vFiler unit is running Data ONTAP version 7.0 or later.

Ensure that the IP address used by the vFiler unit is not configured when you create the vFiler unit.

Have the following information available for the vFiler unit that you want to create:

- Name
- IP space
- Protocols assigned to the vFiler unit (NFS, CIFS, iSCSI)
- IP address
- Name of the storage system or resource pool to be associated with the vFiler unit
- Network mask
- Network interface to use
- VLAN id information (optional in an active/active configuration)
- Partner interface in an active/active configuration (disabled if VLAN id is not provided)
- vFiler template name (optional)
- Windows workgroup name or the CIFS domain user and password
- Root password (optional during vFiler creation)
- Script path (optional)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Click **Add** to start the **Add vFiler Unit** wizard.
3. Enter or select information as requested in the wizard, then click **Finish**.

You can complete the entire vFiler configuration or you can create an inactive vFiler unit and complete the protocol or network setup later.

You can verify that the vFiler unit you added is included in the hosts list in the **vFiler Units** window.

If you provided all of the required information during the create process, you can now protect or provision data that is associated with the new vFiler unit.

If you did not specify all of the vFiler unit information during the creation process, you can configure it later by using the **Setup vFiler Unit** wizard on the **Hosts > vFiler Units** window.

#### **Related concepts**

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Decisions to make before setting up vFiler unit properties

---

Before starting the **Setup vFiler Unit** wizard to configure vFiler storage unit properties, it is useful to have all of the configuration information available for the unit that are you configuring.

Use the vFiler Setup option to add or modify vFiler unit attributes. For example, if you assigned but did not configure the CIFS protocol when you created the vFiler unit, you can use the **Setup vFiler Unit** wizard to perform the CIFS configuration.

<b>Allowed protocols</b>	What assigned protocols do you want to add or change on the vFiler unit?  The following protocols are supported: <ul style="list-style-type: none"><li>• NFS</li><li>• CIFS</li><li>• iSCSI</li></ul>
	Fibre Channel is <i>not</i> supported on vFiler units.
	<b>Attention:</b> If you assign the CIFS protocol to the vFiler unit, you need to set up CIFS before you can use the vFiler unit. Performing the setup stops and restarts CIFS, interrupting the CIFS service.
<b>IP address</b>	What IP address do you want for the vFiler unit?  The IP address accepts both IPv4 and IPv6 address formats.
<b>Network mask</b>	What network mask do you want for the vFiler unit?  <b>Note:</b> The Network mask accepts both IPv4 and IPv6 address formats. When using IPV4 format, use four octet notation. When using IPV6 format, specify the network mask length (the number of bits, from 1 to 127).
<b>Network interface</b>	What Ethernet interface do you want to add or change for the vFiler unit?  The Ethernet interface is not required to create the vFiler unit, although you must specify an interface before you can use the vFiler unit. If you plan to run scripts on the vFiler unit, you might choose to wait to specify the Ethernet interface later, by using the Setup option.
<b>VLAN ID</b>	Do you want to specify a VLAN ID?  VLANs allow you to partition a physical network into multiple virtual networks that are totally separate from one another.

If the vFiler unit that you plan to add is created on an active/active host, you can use an existing VLAN ID or create a new VLAN ID for the vFiler unit.

**Partner interface** What partner interface do you want?

If you are using an active/active host in the setup of the vFiler unit, the partner interface is selected automatically. If no partner interface is configured, then the column is not visible.

The storage system on which the vFiler unit is created must be configured as an active/active configuration before setting up the vFiler unit.

**vFiler template** Which vFiler template do you want?

You must reselect a vFiler template during setup. A vFiler template is a set of vFiler configuration settings and the corresponding CIFS configuration settings.

**Attention:** The **Setup vFiler Unit** wizard does not remember the vFiler template used during the vFiler unit creation. If you do not select the vFiler template you originally used, the network settings are cleared.

**CIFS workgroup name** What Windows workgroup name do you want for the CIFS setup?

The Windows workgroup name specifies the name of the shared resources. The workgroup name option is displayed if the following apply:

- You select the CIFS protocol
- You select the Perform CIFS setup option
- You do not select a vFiler template or the template you select does not include CIFS settings

If you set up the vFiler unit to use the CIFS protocol, the vFiler units can use the same computer names as the servers. This enables CIFS clients to share resources without having to remap their drives or search for the new server.

**CIFS domain user and domain password** What CIFS domain user ID and password do you want?

You can enter a login name and password for administrative access to the Active Directory system. The Domain User and Domain Password options are displayed if the following apply:

- You select the CIFS protocol
- You select the Perform CIFS setup option
- You select a vFiler template that specifies Active Directory for CIFS authentication

<b>Root password</b>	Which vFiler unit root password do you want?  If you did not choose a root password when you created the vFiler unit, you must choose one before you can use the vFiler unit.
<b>Script path</b>	Do you want to use a custom script to help manage vFiler units? If so, what is the full path of the script?  You can use the script while creating or setting up the vFiler unit.  <b>Note:</b> If the DataFabric Manager server is running on Windows, and if the post-setup script for the vFiler unit is on a network share, the script location must be specified by the full UNC path (no drive letter mapping).

### Related tasks

[\*Setting up vFiler unit properties\*](#) on page 935



# Considerations for active/active hosts

---

When using an active/active host in the creation or setup of a vFiler unit, the following are important considerations.

- If you want to use an active/active host in creating your vFiler unit, you need to configure the storage systems before creating the vFiler unit.
- In order to have appropriate failover behavior, you need to configure new IP space and VLAN interface when creating the vFiler unit.
- If you are creating a vFiler unit using non-default IP space, Provisioning Manager moves the partner interface to the non-default IP space of the primary vFiler unit.
- If you are creating a VLAN as part of the vFiler unit creation or setup, a corresponding VLAN will be setup on the partner interface.

## Related concepts

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

## Related tasks

[\*Setting up vFiler unit properties\*](#) on page 935



# Setting up vFiler unit properties

---

After you create a vFiler unit, you can configure the CIFS protocol, if you assigned one, or edit vFiler unit attributes by using the **Setup vFiler Unit** wizard.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available for the vFiler unit that you want to configure:

- Allowed protocols
- IP address
- Network mask
- Network interface
- VLAN ID information (optional in an active/active configuration)
- Partner interface to use in an active/active configuration
- vFiler template name
- Root password
- CIFS Windows Workgroup Name or Active Directory Domain User and Domain Password
- Script path (optional)

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit from the list and click **Setup** to open the **Setup vFiler Unit** wizard.

You can view the current configuration information of the vFiler to ensure that you do not override any information you do not want to change.

3. Modify the vFiler attributes that you want to change.

If you assigned the CIFS protocol to the vFiler unit, select the **Perform CIFS setup** check box to complete the CIFS domain authentication, then enter the appropriate information.

4. Click **Finish**.

You can see your changes in the details section of the **vFiler Units** window.

## Related concepts

*Decisions to make before setting up vFiler unit properties* on page 929

*Considerations for active/active hosts* on page 933

**Related references**

*Administrator roles and capabilities* on page 1055

# Editing storage system properties

---

You can change the login or NDMP credentials of storage systems and you can add licenses to storage systems that are managed by NetApp Management Console . The storage system properties sheet is particularly useful for modifying the credentials for multiple systems at one time.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If you do not have the proper privileges, you cannot select the credentials or licenses in the storage system property sheet.

## Steps

1. From the navigation pane, click **Hosts > Storage Systems** .
2. Select a host name from the host list.

If you have hosts that use the same user name and password, you can select multiple hosts to configure the same credentials on all the selected hosts. License information can only be edited on one host at a time.

3. Click **Edit** to open the properties sheet for the selected host.

You can edit the login credentials and the NDMP credentials for the selected host or add licenses to the host.

4. Verify that the changes you made to the storage system have been implemented.

You can view the properties information provided in the **Storage Systems Hosts** window.

The host credentials are updated in the DataFabric Manager database. It might take several minutes for the updated status to be reflected in the Login Credentials field for each selected host.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Editing Open Systems SnapVault properties

---

You can change the NetApp Host Agent password or the NDMP credentials for the Open Systems SnapVault hosts that are managed by NetApp Management Console.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If you are editing an Open Systems SnapVault host that resides on a VMware® ESX 3.5 server, see the guidelines for editing an Open Systems SnapVault host on a VMware® ESX 3.5 server.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. Select an Open Systems SnapVault host name from the host list.

If you have hosts that use the same user name and password, you can select multiple hosts to configure the same credentials on all the selected hosts.

3. Click **Edit** to open the properties sheet for the selected host.

**Note:** The default NetApp Host Agent user name is "admin", which cannot be changed.

4. Verify that the changes you made to the host have been implemented.

You can view the properties information provided under **Hosts > OSSV**.

The NDMP credentials for the selected host are updated in the DataFabric Manager database. It might take several minutes for the updated status to be reflected in the NDMP Credentials field for the selected host.

## Related references

- [Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#) on page 919  
[Administrator roles and capabilities](#) on page 1055



# Stopping Open Systems SnapVault agents

---

You can stop the Open Systems SnapVault agent to perform maintenance on one or more selected clients or to reconfigure Open Systems SnapVault. When troubleshooting protection errors on a client running Open Systems SnapVault, stopping and then restarting the Open Systems SnapVault agent might solve the problem.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

There is no Open Systems SnapVault plugin for Solaris. Therefore, management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console on Solaris systems.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients on which you want to stop Open Systems SnapVault services.
3. Click **Stop**.

**Note:** Stopping the Open Systems SnapVault agent on a client causes the backup service on that client to stop. Be sure to restart the agent if you want to resume backup protection.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Starting Open Systems SnapVault agents

---

When you are troubleshooting protection errors on a client running Open Systems SnapVault, stopping and then restarting the Open Systems SnapVault agent might solve the problem.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

There is no Open Systems SnapVault plugin for Solaris. Therefore, management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console on Solaris systems.

If you stop Open Systems SnapVault services to troubleshoot a problem or to perform maintenance, be sure to restart the Open Systems SnapVault agent when you are ready to resume services.

## Steps

1. From the navigation pane, click **Hosts ▶ OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients on which you want to start or resume Open Systems SnapVault services.
3. Click **Start**.

The Open Systems SnapVault agent starts on each selected client, and backup service starts or resumes on each client according to its schedule.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Updating Open Systems SnapVault client data

---

Data shown in the list of Open Systems SnapVault clients is gathered at regular intervals. If you are trying to troubleshoot a problem with an Open Systems SnapVault client, you can update the data for that client as needed to view the most current status.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients for which you want to update data.
3. Click **Refresh**.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Diagnosing a storage system

---

You can use the **Diagnose Storage Systems** wizard to verify the configuration for your storage system. You can also make necessary changes to some of the storage system properties and enable SnapMirror and SnapVault licenses from the diagnostics wizard.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

When running the diagnostics wizard, it can be useful to have the following information available to verify for the storage system that you want to diagnose:

- Host Name
- Domain Name
- IP Address
- Licenses that should be enabled for the storage system
- SnapMirror Access Control List for the storage system, if licensed for SnapMirror
- SnapVault Access Control List for the storage system, if licensed for SnapVault
- Login Credentials (user name and password)
- NDMP Credentials (user name and password)

**Note:** The credentials of a vFiler unit always have a status of Not Applicable. This status for a vFiler unit does not indicate a problem.

## Steps

1. From the navigation pane, click **Hosts ▶ Storage Systems**.
2. Click **Diagnose** to start the wizard, then verify or modify information as requested in the wizard.

The diagnostics wizard checks the configuration of hosts.
3. Verify that any changes that you made to your host configuration are displayed in the storage systems list in the **Storage Systems Hosts** window.

If configuration changes are made to a host from an interface other than NetApp Management Console , you might need to use the Refresh button to pull those changes into the host list for viewing in the console.

## Related concepts

[Ways to investigate problems with hosts](#) on page 903

**Related references**

*Administrator roles and capabilities* on page 1055

# Diagnosing an Open Systems SnapVault host

---

You can use the **Diagnose OSSV Host** wizard to verify your Open Systems SnapVault configuration and to make necessary changes to some Open Systems SnapVault properties.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

When running the diagnostics wizard, it can be useful to have the following information available to verify for the Open Systems SnapVault host that you want to diagnose:

- Host Name
- Domain Name
- IP Address
- NetApp Host Agent port number
- Operating system credentials for the host on which NetApp Host Agent is running, if you would like to use DataFabric Manager to update and manage the credentials for you
- NDMP Credentials (user name, password, and port number)

## About this task

When diagnosing issues on Solaris systems, note that there is no Open Systems SnapVault plugin for Solaris, so the NetApp Host Agent cannot talk to the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. Click **Diagnose** to start the wizard. Verify or modify information as requested in the wizard.
3. Verify that any changes you made are displayed in the hosts list in the **OSSV Hosts** window.

You might need to refresh the window before you can view the changes in the hosts list.

## Related concepts

[Ways to investigate problems with hosts](#) on page 903

## Related references

[Administrator roles and capabilities](#) on page 1055



# vFiler unit migration overview

---

You can migrate a vFiler unit to another storage system. If your storage strategy is focused on vFiler units as containers for datasets; you can migrate a vFiler unit when one or more datasets are completely contained by that vFiler unit.

## Related concepts

[\*Description of migration tasks\*](#) on page 955



## vFiler unit migration requirements

---

A vFiler unit must meet the following requirements before you can migrate it to another vFiler unit.

- A vFiler unit that has its root storage as a qtree in a volume that is not owned by the vFiler unit can be migrated. However, the backup Snapshot copies of that qtree cannot be migrated.
- The vFiler unit cannot have volumes that are destinations of backup or mirror relationships.
- All qtrees contained by the vFiler unit must be in a volume that belongs to the vFiler unit. The exception is a qtree that contains root storage for the vFiler unit.
- The vFiler unit must be running Data ONTAP release 7.3.1 or later.



# Description of migration tasks

---

A complete migration of a dataset or vFiler unit includes all of the following operations. Each operation can be initiated separately on the **Datasets** window Migration tab or on the **vFiler Units** window.

## Next topics

- [\*Migration Step 1. Start\* on page 956](#)
- [\*Migration Step 2. Update \(optional\)\* on page 956](#)
- [\*Migration Step 3. Cutover\* on page 957](#)
- [\*Migration Step 4. Cleanup\* on page 958](#)
- [\*Manual cleanup after migration\* on page 958](#)

## Related concepts

- [\*vFiler unit migration overview\* on page 951](#)
- [\*Decisions to make before starting vFiler unit migration\* on page 959](#)
- [\*Dataset migration overview\* on page 769](#)
- [\*Dataset migration limitations\* on page 775](#)
- [\*Decisions to make before starting dataset migration\* on page 781](#)

## Related tasks

- [\*Starting a vFiler unit migration\* on page 961](#)
- [\*Updating vFiler unit migration SnapMirror relationships\* on page 963](#)
- [\*Cutting over to the new vFiler unit destination\* on page 965](#)
- [\*Cleaning up a vFiler unit migration\* on page 967](#)
- [\*Starting a dataset migration\* on page 783](#)
- [\*Updating dataset migration SnapMirror relationships\* on page 785](#)
- [\*Cutting over to the new dataset storage destination\* on page 787](#)
- [\*Cleaning up a dataset migration\* on page 789](#)

## Migration Step 1. Start

This operation begins data migration by starting the **Dataset Migration** wizard or the **vFiler Unit Migration** wizard, which starts a baseline transfer of the data to a new destination.

The licensed provisioning application performs the following tasks:

- Checks the destination storage system for the following:
  - The storage system has licenses for SnapMirror, MultiStore, and for all the allowed protocols of the source vFiler unit.
  - The vFiler unit limits for the storage system are not at a maximum level.
  - There are no name conflicts for all the source volumes.
  - There is space available for all the source volumes.
- Provisions destination storage according to the destination provisioning policy.  
For vFiler unit migrations in which the vFiler unit is a container of one or more datasets, the destination is provisioned according to the respective provisioning policies for each dataset.
- Creates the required IPspace and VLANs on the destination storage system.
- Starts the vFiler unit migration by starting the baseline transfer of the vFiler unit volumes.
- Polls for the SnapMirror transfers to complete.

If the provisioning application encounters a failure at any point in this operation, it undoes the entire process and reports the error.

## Migration Step 2. Update (optional)

This operation performs an on-demand update of the SnapMirror relationships that were created as part of the migration start operation. This operation is useful if a scheduled update fails, which causes the lag time of the SnapMirror relationships to increase to an undesirable length.

## Migration Step 3. Cutover

This operation stops access to the VFiler unit on the source storage system from which the data is served and enables access to the vFiler unit on the new destination storage system. You must shut down all applications using the dataset or vFiler unit before beginning the migration cutover operation.

Before performing the data source cutover to the new destination, the provisioning application verifies that the following is true:

- The IP addresses of the source vFiler unit are not in use in the same IPspace in the destination storage system.
- No error occurred in the last SnapMirror update on any of the SnapMirror relationships involved in migration.
- The destination storage system has the licenses for all allowed protocols on the vFiler unit.
- The aggregates hosting the destination volumes have enough space.
- All the volumes belonging to the source vFiler units or units have SnapMirror relationships to the destination volumes.

If any of these items is not true, the cutover of the data source to the new destination is not performed and an error is reported.

When all checks have passed, the provisioning application performs the following tasks:

- Runs the specified script
  - If a script is specified as part of the destination switch operation and it contains premigration operations, they are executed before the cutover is performed.
    - If a script is specified as part of the destination switch operation and it contains cutover operations, they are executed during the cutover operation. (This is useful when you have a script to quiesce an application.)
      - If the script contains postmigration operations, they are executed after the cutover is performed. (This is useful when you have a script to resume an application.)
  - Switches data access from the original source vFiler unit to the new destination VFiler unit and deletes the source vFiler unit.
    - The new destination vFiler unit becomes active, writable, and online.
- Suspends the datasets
  - This prevents new backups from starting during the migration.
- Removes volumes from the source dataset
  - As each volume is added to the new destination, the source volume is removed from the source dataset. Dynamic references in the source dataset are not removed; you must remove them manually after the migration cleanup operation finishes.
- Modifies the backup version tables to point to the new primary storage.
- Modifies all backup and mirror relationships to point to the new primary storage.

- Copies the history data in Operations Manager to reflect the new primary storage.
- Resumes the dataset operation.

When these tasks are finished, you can restart any applications that were shut down before the migration.

The provisioning application responds to failures as follows:

- If the data migration succeeds but the backup relationship migration fails, the dataset remains in suspended mode with the status Migrated-Errors.  
You must manually correct the errors. When the errors are corrected, you can use the Operations Manager CLI commands to change the migration status to Normal and then resume dataset operation.
- If the migration cutover operation fails, the source vFiler unit is brought back online, the status of the source dataset and vFiler unit is set to Migrate-Failed, and the destination storage is destroyed.

## **Migration Step 4. Cleanup**

This operation deletes the volumes that were used by the vFiler unit on the old data storage system. A preview window allows you to see which volumes will be destroyed. VLANs and IPspaces used by the old vFiler unit are not automatically destroyed; you must remove them manually after the migration cleanup operation finishes.

## **Manual cleanup after migration**

After all migration cleanup operation has finished successfully and the dataset or vFiler unit status has the status "Not started," you must use an application like FilerView to manually delete the following:

- Dynamic references in the old, source dataset.
- VLANs and IPspaces used by the old, source vFiler unit.

# Decisions to make before starting vFiler unit migration

---

Before you start a vFiler unit migration by using the **vFiler Unit Migration** wizard, it is useful to have ready all the migration information for the vFiler unit.

- |   |   |
|---|---|
| <b>Dataset migration commands or vFiler unit migration commands</b> | Are you migrating a dataset or a vFiler unit? <ul style="list-style-type: none"><li>• If there is a direct one-to-one correspondence between a dataset and a vFiler unit, you may use either the dataset migration commands or the vFiler unit migration commands.</li><li>• If a vFiler unit contains more than one dataset, and the storage for each dataset is completely owned by the vFiler unit, you should use the vFiler unit migration commands.</li><li>• If a vFiler unit contains more than one dataset, but the storage for at least one of the datasets is owned by more than one vFiler unit, you should use the dataset migration commands for each separate dataset.</li></ul> |
|---|---|

- |                                   |  |
|-----------------------------------|--|
| <b>Destination storage system</b> | What is the destination storage system for the migrated vFiler unit?<br>The wizard displays a list of the storage systems, from which you can select the destination storage system. |
|-----------------------------------|--|

**Note:** Because you can select storage systems that are not in the resource pool, the vFiler unit might not be in conformance after the migration. To avoid nonconformance, you can add the storage system to the resource pool before starting the migration.

- |                             |  |
|-----------------------------|--|
| <b>Interface selections</b> | What interfaces do you want to use?<br>You can select from a list of prepopulated IP addresses that displays the associated Netmask and Interface values and the prepopulated VLAN ID for each. Or you can modify the IP addresses and VLAN IDs, or you can add additional ones. |
|-----------------------------|--|

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Starting a vFiler unit migration](#) on page 961



# Starting a vFiler unit migration

---

You can begin migration of a vFiler unit by initiating the migration start operation, which starts the **vFiler Unit Migration** wizard and performs the first set of operations for the migration.

## Before you begin

Have available the information that you need to complete this task:

- Destination storage system (required)
- Interface to which the IP address will be bound to the destination storage system and the VLAN ID (required)
- Physical VLAN interface on which the VLAN will be created if VLANs are created during migration for the partner of the destination storage system (required if the destination storage system has an active/active configuration)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can cancel a vFiler unit migration anytime during the migration start operation.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Start migration** to start the **vFiler Unit Migration** wizard.
3. Complete the steps in the wizard to start the migration.

On the Interface Selection page of the wizard, you can specify a VLAN ID to create a tagged interface. However, you can tag only the base interfaces that are down.

To add more interfaces, click **Add**. To delete an interface, select it and click **Delete**.

You can check the job progress displayed in the Tracking Dataset Migration Job display popup window or you can move the popup window to the background and track the job progress in the **Jobs** window.

At any time after the migration start operation finishes successfully, you can update the SnapMirror relationships by initiating the migration update operation.

## After you finish

To continue the migration, you must manually initiate the migration cutover operation.

## **Related concepts**

[\*Decisions to make before starting vFiler unit migration\*](#) on page 959

[\*Description of migration tasks\*](#) on page 955

## **Related tasks**

[\*Updating vFiler unit migration SnapMirror relationships\*](#) on page 963

[\*Cutting over to the new vFiler unit destination\*](#) on page 965

[\*Canceling a vFiler unit migration\*](#) on page 969

## **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Updating vFiler unit migration SnapMirror relationships

---

After the migration start operation finishes, you can initiate an on-demand update of the SnapMirror relationships that were created as part of the migration start operation. This is an optional step in the vFiler migration process.

## Before you begin

You can perform this task only on a vFiler unit that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

This operation is useful if a scheduled update fails, which causes the lag time of the SnapMirror relationships to increase to an undesirable length. The migration

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Update** to update the SnapMirror relationships that were created as part of the migration start operation.
3. Click **Yes** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Jobs** window.

## After you finish

To continue the migration, you must manually initiate the migration cutover operation at a convenient time.

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Starting a vFiler unit migration](#) on page 961

[Cutting over to the new vFiler unit destination](#) on page 965

**Related references**

*Administrator roles and capabilities* on page 1055

# Cutting over to the new vFiler unit destination

---

After the migration start operation finishes, you can initiate the migration cutover operation to switch the old destination from which the data is served to the new destination and update the SnapMirror relationships.

## Before you begin

- You can perform this task only on a vFiler unit that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.
- Because this is an automated offline migration, you must shut down all applications that use the vFiler unit.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You might want to initiate this operation at a time when the vFiler unit has a very low level of activity. When the migration cutover operation begins, you cannot cancel or reverse it.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Cutover**.
3. (Optional) In the confirmation dialog box, you can enter the name of a script to be executed.

For example, a script might quiesce an application and then resume the application.

4. Click **Cutover** in the confirmation dialog box to begin the operation.

After access to the data is switched over to the vFiler unit on the destination storage system, the backup versions, backup relationships, and DataFabric Manager history for the volumes are transferred to the destination storage system.

## After you finish

- To continue the migration, you must manually initiate the migration cleanup operation.
- You must restart all applications that use the data owned by the migrated vFiler unit.

## Related concepts

[Description of migration tasks](#) on page 955

## **Related tasks**

[\*Starting a vFiler unit migration\*](#) on page 961

[\*Updating vFiler unit migration SnapMirror relationships\*](#) on page 963

[\*Cleaning up a vFiler unit migration\*](#) on page 967

## **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Cleaning up a vFiler unit migration

---

After the migration cutover operation finishes, you can initiate the migration cleanup operation to delete the old storage.

## Before you begin

You can perform this task only on a vFiler unit that has the status "Migrated, cleanup required." This status indicates that the migration cutover operation is finished and access to the data is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. However, old storage needs to be deleted.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Cleanup**.

The Migration Cleanup confirmation dialog box lists the volumes on the old destination that will be deleted.

3. Click **Apply** in the confirmation dialog box to begin the operation.

## After you finish

To complete the migration process, you must manually perform the following cleanup tasks using an application like FilerView (if the VLANs and IPspaces are not shared):

- Delete dynamic references in the old source dataset.
- Delete VLANs and IPspaces used by the old source vFiler unit.

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Cutting over to the new vFiler unit destination](#) on page 965

## Related references

[Administrator roles and capabilities](#) on page 1055



# Canceling a vFiler unit migration

---

You can cancel a vFiler unit migration at any time when the status is "started, cutover required." When you cancel a vFiler unit migration, the licensed provisioning application aborts all ongoing transfers and deletes all the provisioned storage on the destination storage system and on the destination vFiler unit.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Click **Cancel**.
3. In the confirmation dialog box, click **Yes**.

## After you finish

After you cancel a vFiler unit migration, you must manually delete the VLANs and IPspaces that were created on the destination storage system and vFiler unit.

## Related tasks

[Starting a vFiler unit migration](#) on page 961

## Related references

[Administrator roles and capabilities](#) on page 1055



# Viewing vFiler unit migration status

---

You can view the status of a vFiler migration operation in the **vFiler Units** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Step

1. From the navigation pane, click **Hosts > vFiler Units**.

The status is displayed in the "Migration status" column.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Overview of resource pools

---

A resource pool is a collection of unused physical storage resources, such as aggregates and disks, grouped together based on a user-defined set of common attributes.

You might pool your resources based on attributes such as performance, cost, physical location, or availability. By grouping related resources into a pool, you can treat the pool as a single unit for monitoring, provisioning, reporting, and role based access control (RBAC). This simplifies the management of these resources and allows for a more flexible and efficient use of the storage.

You create resource pools by using the **Add Resource Pool** wizard, which is accessible from the **Resource Pools** window. By using the wizard, you can select from a list of available aggregates, entire storage systems, or groups of physical resources from which to create your resource pool.

After you create a resource pool, you can associate it with one or more datasets. You can also associate datasets with provisioning and protection policies. These tasks can be accomplished when you add or edit datasets from the **Datasets** window.

When you assign a data protection policy, the licensed protection application applies the policy settings to automatically provision destination volumes from the assigned resource pool. It then creates backup and mirror relationships from each volume and qtree in the dataset to the newly provisioned secondary storage.

When you assign a provisioning policy to a dataset node, the licensed provisioning application applies the availability characteristics and space settings in the policy to automatically select the resources needed to fulfill a request for storage space for the primary data of a dataset.

These relationships between physical storage units, resource pools, and datasets mean that you must consider carefully what the impact might be of changes made to the system.

## Related concepts

[Dataset concepts](#) on page 693

[Decisions to make before adding datasets](#) on page 711

[Ways you might combine resources in resource pools](#) on page 825

[What groups are](#) on page 1047

[Decisions to make before assigning or changing policies](#) on page 721

**Related references**

*Advantages of using resource pools* on page 821

# Advantages of using resource pools

---

By using resource pools, you can simplify physical storage resource management in several ways.

Some advantages of using resource pools are listed here:

- You can group various resources with similar attributes, providing a quick view of similar storage objects.
- Resource pools provide a single logical unit for provisioning.
- You can simplify physical resource management by managing a pool of resources as a single entity.
- You can configure your system to automatically provision storage from resource pools, without your intervention.
- You can create resource pools in advance of allocating them to datasets, so that the resource pools are available when needed.
- You can enable event generation on resource pools so that when a set threshold is crossed, an event is generated to alert the resource pool owner.
- You can assign a label to resource pools or members of resource pools.

This allows you to filter the resources available for provisioning to only those that have a specific label assigned to them.

**Note:** This feature is available only when the provisioning application is licensed.

## Related concepts

[\*Overview of resource pools\*](#) on page 819

[\*Ways you might combine resources in resource pools\*](#) on page 825



# Resource pool properties

---

You can use the following definitions when you configure or edit a resource pool's properties.

- [General Properties](#) on page 823
- [Physical Resources](#) on page 823
- [Labels](#) on page 824
- [Space Thresholds](#) on page 824

## General Properties

These properties are associated with the entire resource pool.

<b>Name</b>	The name assigned to a resource pool. Special characters and spaces are permitted in names. The limit is 64 characters, but for readability, it is best to keep the description under 25 characters
<b>Description</b>	A description of the resource pool. This description might include the intended use of the resource pool, the type of storage contained in the resource pool, or some other common attribute that identifies why the storage was grouped into a resource pool.  The limit is 255 characters, but for readability, it is best to keep the description under 40 characters.
<b>Owner</b>	The name of the person responsible for this resource pool. You can list multiple owners, delimited by commas. There is no formatting restriction.
<b>Contact (optional)</b>	The e-mail address of the person to contact if there are issues with the resource pool. You can have multiple e-mail contacts delimited by commas.
<b>Time Zone</b>	The time zone you want to assign to the resource pool.

## Physical Resources

These properties let you designate which available physical resources to include in this resource pool.

<b>Available physical resources</b>	A list of the physical resources available for assignment to this resource pool.
<b>Resources in this resource pool</b>	A list of physical resources already assigned to this resource pool.

## Labels

These optional properties let you assign optional labels to the resource pool or objects within the resource pool.

<b>Resource Label (optional)</b>	A user-assigned label associated with a resource pool or the objects in a resource pool. It essentially functions as a filter, allowing you to identify specific resources to be considered when fulfilling a provisioning request. A resource label is a text string of any length.
<b>Resources (optional)</b>	The names of the physical storage resources, such as hosts and aggregates, that are allocated to a resource pool.

## Space Thresholds

These optional properties let you designate space usage thresholds at which to generate events and send alarms related to this resource pool.

<b>Space Thresholds (optional)</b>	<p>Resource pool-related data storage measurements at which an event is generated.</p> <ul style="list-style-type: none"><li>• Resource Pool Nearly Full threshold and Resource Pool Full threshold These are thresholds used to track the amount of space consumed in a resource pool. Alerts are generated when these thresholds are reached. The default thresholds are: Nearly Full = 80%, Full = 90%</li><li>• Aggregate Nearly Overcommitted threshold and Aggregate Overcommitted threshold These are thresholds used to track the sum of committed space of all aggregates belonging to the resource pool. Alerts are generated when these thresholds are reached. Tracking these thresholds in an environment where the aggregates are overcommitted (thin provisioning) is particularly important, because in such an environment administrators commit more storage than is physically available. The default thresholds are: Nearly Overcommitted = 300%, Overcommitted = 400%</li></ul>
--	--

## Related tasks

[Adding a resource pool](#) on page 841

[Editing resource pool properties](#) on page 845

## Related references

[Resource pool guidelines](#) on page 831

# Ways you might combine resources in resource pools

---

Prior to creating resource pools, consider how you will be using the available storage. This will help you to determine how you want to combine those resources into resource pools to meet your setup's replication needs.

Following are examples of ways that you might combine your physical resources to make the most efficient use of your resource pools:

- A set of aggregates composed of inexpensive, slow, ATA drives  
This pool is suitable for archival or compliance purposes, but it is not appropriate for mission-critical, high-performance database applications.
- A set of high-performance aggregates composed of 15K Fibre Channel disk drives in a RAID-DP configuration  
This pool is suitable for enterprise-critical applications.
- A set of resources categorized based on cost or performance  
This pool might be given a simple designation, such as *Gold*, *Silver*, or *Bronze*.
- A set of storage systems that are suitable for provisioning for certain departments within an organization
- A set of homogenous resources grouped together as a way of restricting access to high-performance storage

## Related concepts

[Overview of resource pools](#) on page 819

## Related references

[Advantages of using resource pools](#) on page 821



## **Sequence for selecting backup destination volumes**

---

If an existing backup relationship already has a volume assigned to contain backup data, the licensed protection application tries to use it. Otherwise, the application selects an existing volume that meets certain requirements or, if necessary, provisions a new destination volume.

For data residing on storage systems, the size estimate for destination volumes that are provisioned by the protection application is 1.2 times the size of the volume containing the protected data. The destination aggregate must have at least this much available space.

**Note:** Whenever possible, the protection application uses FlexVol volumes when provisioning backup destination volumes. The application implements aggregate overcommitment, observing the Aggregate Overcommitted and Aggregate Nearly Overcommitted thresholds specified in Operations Manager. For more information about aggregate overcommitment, see the *Operations Manager Administration Guide* and the *Data ONTAP Storage Management Guide*. For information about the aggregate overcommitment thresholds, see the Operations Manager online Help.

For data residing on Open Systems SnapVault clients, the licensed protection application uses a projected size of 100 GB for the destination volume.

To be considered as a destination for backups, a volume must be on a storage system configured with the appropriate Data ONTAP licensing to store backups.

From the pool of volumes that meet these requirements, the protection application takes the following steps to select a destination volume for backups:

1. The application looks for secondary volumes associated with the dataset that already have a relationship originating from the primary volume.  
However, if a secondary volume has too many relationships, the application excludes that volume from the selection process. The default maximum number of relationships is 50.
2. Of the secondary volumes associated with the dataset that have a pre-existing relationship with the primary volume, the application looks for a destination that has enough space to satisfy the projected space requirement of the primary data.
3. If none of the secondary volumes with pre-existing relationships with the primary volume can satisfy the space requirement, the application scans the destination systems for an existing FlexVol volume with adequate space and no SnapVault or Qtree SnapMirror relationships.
4. If the protection application cannot locate an existing FlexVol volume with adequate space and no SnapVault or Qtree SnapMirror relationships, it scans the destination systems for existing traditional volumes with adequate space and no SnapVault or Qtree SnapMirror relationships.
5. For systems running Data ONTAP 7.0 or later, if the protection application cannot find a volume with adequate space and no existing SnapVault relationships, it attempts to provision a FlexVol volume.
6. If the application cannot provision a FlexVol volume, it generates an error.

**Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## **Sequence for selecting mirror destination volumes**

To find a suitable destination to contain mirrored data, the licensed protection application tries to use the same volume used for the existing mirror relationship, if there is one. Otherwise, the application selects an existing volume that meets certain requirements or, if necessary, provisions a new destination volume.

If the protection application needs to provision a new volume to contain mirrored data, the new volume is provisioned to be the same size as the aggregate in which it resides.

**Note:** If the application provisions a mirror destination volume on a tertiary node, the new volume is provisioned to be the same size as the secondary volume even if the secondary volume is larger than the tertiary aggregate. Space guarantees for the new volume are disabled.

The licensed protection application takes the following steps to select a destination volume for mirror copies:

1. If there is no existing mirror relationship, the application scans the destination systems for an existing volume that meets the following requirements:
  - Is located on a storage system running the same or later Data ONTAP version as the storage system containing the data to be mirrored
  - Is located on a storage system on which the SnapMirror license is enabled
  - Is of the same type (FlexVol or traditional volume) as the volume containing the data to be mirrored
  - Is the same size or larger than the source volume
  - Has no SnapVault or SnapMirror relationships
2. If the application cannot locate an existing volume that meets the preceding requirements, it attempts to use available space in the resource pool to provision a new volume of the same type as the volume containing the data to be mirrored. For the protection application to provision a new volume, the aggregate or spare disk where the new volume is created must meet the following requirements:
  - Belongs to a storage system running the same or later Data ONTAP version as the storage system containing the data to be mirrored
  - Belongs to a storage system on which the SnapMirror license is enabled
  - Has adequate space for the data in the source volume
3. If the application cannot provision a new volume for the data to be mirrored, it generates an error.



# Resource pool guidelines

---

These guidelines can help you optimize the advantages of using resource pools.

## Content and structure of resource pools

- Resource pools cannot nest and cannot overlap (that is, storage in one resource pool cannot be in another resource pool).
- Resource pools can be members of DataFabric Manager groups, but resource pools cannot contain DataFabric Manager groups.
- Resource pools can be created from entire storage systems or from aggregates.
- Adding a storage system to a resource pool implies that all existing aggregates and spare disks on the storage system are included as part of that pool, along with any new aggregates that are created.
- Members of a resource pool do not all need to reside on the same storage system or .
- A storage system can be designated as a resource pool that contains a mixture of resources with various attributes.
- A storage system or an aggregate can only belong to one resource pool at a time.
- Individual aggregates within the same storage system can belong to different resource pools as long as the storage system as a whole has not been assigned to a resource pool.

## Considerations when selecting storage for resource pools

- When creating a resource pool, you determine which storage elements to include in the pool based on one or more common properties, such as "all storage in the same building" or "all storage delivering the same level of performance."
- Adding an aggregate to a resource pool allows the application to create new volumes by using the aggregate's free space.  
When provisioning resources, the aggregate's preexisting volumes are not used.
- When provisioning resources for primary data, you can choose to increase the available space in an existing volume by deleting Snapshot copies or by assigning additional space for the volume. LUNs cannot be resized.  
In a NAS environment, space can be grown and Snapshot copies deleted only manually. In a SAN environment, these tasks can be done manually, but they can also be done automatically by using a provisioning policy.
- Access to a resource pool is controlled via role-based access control (RBAC), so in some deployments you might want to group homogeneous resources together as a way of restricting access to high performance storage. In other deployments you might construct resource pools with a mix of storage attributes as a means of providing better storage utilization across an organization.

- Systems running on Data ONTAP versions earlier than 7.0 cannot use the aggregate or flexible volume features. This impacts how you assign destination resources for mirrored copies and backups.

**Mirrors** If you are mirroring data, you can only select entire storage systems to include in resource pools. The licensed protection application uses the spare disks on the storage systems to provision traditional volumes for the mirrored copies.

**Backups** The licensed protection application cannot provision resources for backup jobs. You must, manually create the volumes to add to the dataset's secondary node. When you assign resources to a dataset, only the volumes are available for selection.

#### **Provisioning from resource pools**

- When a resource pool contains a storage system, all aggregates on the storage system are available for provisioning.
- Both traditional and flexible volumes can be created from a resource pool. However, flexible volumes are available only when running systems on Data ONTAP 7.0 or later.
- Aggregates are used for provisioning of flexible volumes for Data ONTAP 7.0 or after. Spare disks are used for provisioning of traditional volumes by the administrator, for Data ONTAP versions prior to 7.0.
- When using the licensed protection application, you cannot control how specific volumes are provisioned from resource pools. The application evaluates available resources for a number of criteria, such as valid login credentials, working NDMP, ONTAP version, licenses, and so forth. From the aggregates that pass those filters, the application picks the aggregate with the most free bytes as the one to hold the backup.

#### **Naming and labeling resource pools**

- You are advised to name resource pools according to the characteristics of the storage each resource pool contains.
- The name is limited to 64 characters. However, for readability, it is advised that names be no longer than 25 characters. You can use any combination of letters, numbers, or special characters in resource pool names.
- Use a label name that has significant meaning. A label should only be used when you want to more narrowly control the resources being provisioned. For example, if you want to restrict the provisioned resources by their cost and performance, you might assign a label of Tier-1, Tier-2, or Tier-3. If a Tier-1 resource label is selected for a provisioning policy and a provisioning action occurs, only those resources assigned to the dataset and labeled as Tier-1 will be considered for provisioning.

**Note:** The Label property is only available when the provisioning license is installed.

**Status of resource pools** The status of a resource pool is equivalent to the worst status of any event pools associated with any member of that resource pool.

#### Related concepts

*[Decisions to make before adding a resource pool](#)* on page 837

#### Related tasks

*[Adding a resource pool](#)* on page 841

*[Editing resource pool properties](#)* on page 845

#### Related references

*[Resource pool properties](#)* on page 823



## How resource labels work

---

You can assign a resource label as a way to narrow the available resources to be considered for a provisioning request. This feature is only available when the provisioning application is licensed.

The resource label can be assigned when you create a resource pool. This is an optional custom property that you can assign to a resource pool or to the individual storage systems or aggregates that comprise the resource pool. You might assign a resource label based on factors such as cost, reliability, or specific configurations. The resource label essentially functions as a filter. It allows you to identify specific resources to be used to fulfill a provisioning request, so that only those resources that have the label assigned to them are considered. This allows finer control when matching provisioning requests with available resources.

When you create a provisioning policy, you can specify a resource label to be associated with the policy. If a label is specified for a policy, only the resource pools and resource pool members that match the label are used when a provisioning request is fulfilled using that policy. However, storage that has an assigned resource label can still be used to fulfill provisioning requests that do not specify a label.

For example, assume an administrator assigns a resource label of **Tier-1** to a resource pool containing the highest-cost, most reliable storage. The administrator also creates a provisioning policy named prov-pol-1, with the resource label **Tier-1** specified. When a provisioning request is made on a dataset that has the prov-pol-1 policy assigned to it, the provisioning application searches for storage that uses the **Tier-1** label. If no resources with that resource label are available, the provisioning request fails. For this reason, you should use resource labels with care.



## Decisions to make before adding a resource pool

---

Before creating a resource pool by using the **Add Resource Pool** wizard, it is useful to have all the resource pool configuration information ready.

- |                                   |  |
|-----------------------------------|--|
| <b>Name<br/>(required)</b>        | What name do you want to assign to the resource pool? <ul style="list-style-type: none"><li>• Provide a meaningful name that briefly describes the storage or the intended use of the storage in the resource pool.<br/>An example of a name that describes the storage path is: <code>server1_homedirs</code>, <code>tier1_mktg</code>, or <code>china_eng</code>.</li><li>• Special characters and spaces are permitted in names.<br/>The limit is 64 characters, but for readability, it is advised that you keep the name under 25 characters.</li></ul> |
| <b>Description<br/>(optional)</b> | How do you want to describe the resource pool, so the intended use of the resource pool is clear? <ul style="list-style-type: none"><li>• Provide a meaningful description of the resource pool, such as an explanation of the intended use of the resource pool.</li><li>• The limit is 255 characters, but for readability, it is advised that you keep the description under 40 characters.</li></ul>   |
| <b>Owner<br/>(optional)</b>       | Who should be contacted regarding problems with the resource pool? <ul style="list-style-type: none"><li>• Provide the name of the person or people responsible for maintaining this resource pool.</li><li>• You can list multiple owners, delimited with a comma. There is no formatting restriction.</li></ul>  |
| <b>Contact<br/>(optional)</b>     | Who should be alerted regarding problems with the resource pool? <ul style="list-style-type: none"><li>• Provide the e-mail addresses or e-mail aliases to which notifications, alerts, and so forth should be sent concerning the resource pool.</li><li>• The e-mail addresses listed here might be the same ones used for receiving alerts regarding the resource pool.</li><li>• You can have multiple e-mail contacts, delimited with a comma.</li></ul>  |
| <b>Time Zone<br/>(required)</b>   | Will you use the default time zone for the resource pool or change the time zone? <ul style="list-style-type: none"><li>• The resource pool must have a time zone selected. You can retain the default setting or change it.</li></ul>   |

To select a time zone, you can either scroll through the entire list or type a time zone designation in the Filter Time Zone text box.

<b>Physical Resources (required)</b>	<p>How will you determine which storage to include in the resource pool from the list of physical resources available?</p> <ul style="list-style-type: none"><li>Decide on which properties you want to base the creation of the resource pool: for example, location, cost, performance, reliability, or access privileges.</li><li>Decide whether the resource pool will contain individual aggregates, an entire storage system (all the aggregates in a storage system), or a combination.</li><li>Decide which version of Data ONTAP will run on the systems in this resource pool.<ul style="list-style-type: none"><li>Note that systems running Data ONTAP versions earlier than 7.0 cannot use the aggregate or flexible volume features. This impacts how you later assign destination resources for mirror copies and backups.</li></ul></li><li>Decide if you want to use traditional volumes or flexible volumes in the resource pool.<ul style="list-style-type: none"><li>Flexible volumes are available only when running Data ONTAP 7.0 or later.</li><li>Aggregates are used for provisioning of flexible volumes, and spare disks are used for provisioning of traditional volumes.</li><li>If you intend to associate a resource pool with a data set in a mirror relationship, the volumes on the primary node and those on the secondary nodes must be of the same type. You cannot combine traditional volumes and FlexVol volumes on nodes that are part of a mirror relationship.</li></ul></li><li>Decide how much available storage space you need for the resource pool, based on the resource pool's intended use.</li><li>Verify that you have the appropriate software licenses on the storage you intend to use.</li></ul>
<b>Labels (optional)</b>	<p>When a provisioning request is processed, do you want to restrict the resources available for provisioning to only those with a specific label assigned to them?</p> <ul style="list-style-type: none"><li>A label set on an individual member of a resource pool takes priority over a label applied to the entire resource pool.</li><li>The labels can be edited inline in the table. For both resource pool and members, an existing label can be selected from the drop-down list or a new label can be typed in.</li></ul>

<b>Space Thresholds (optional to modify default)</b>	<p>At what point do you want to receive alerts regarding consumption of space in the resource pool?</p> <ul style="list-style-type: none"><li>• Resource Pool Nearly Full threshold and Resource Pool Full Threshold This set of thresholds can be used to track the amount of space consumed in a resource pool. Alerts are generated when these thresholds are reached.</li><li>• Aggregate Nearly Overcommitted threshold and Aggregate Overcommitted threshold This set of thresholds can be used to track the sum of committed space of all aggregates belonging to the resource pool. Alerts are generated when these thresholds are reached. Tracking these thresholds in an environment where the aggregates are overcommitted (thin provisioning) is particularly important, because in such an environment administrators commit more storage than is physically available.</li></ul>
--	---

#### Related concepts

[\*Effect of time zones on schedules\*](#) on page 1049

[\*Protection policy node prerequisites\*](#) on page 1051

#### Related tasks

[\*Adding a resource pool\*](#) on page 841

#### Related references

[\*Resource pool guidelines\*](#) on page 831



# Adding a resource pool

---

You can create resource pools from collections of unused physical storage resources. Resource pools are associated with one or more datasets, providing the physical resources for provisioning primary storage by using a provisioning policy and also for backup or mirror protection on nonprimary nodes.

## Before you begin

Ensure that the hosts you are adding to the resource pool have the proper configuration and licensing for their intended use.

Have the information available that you need to complete this task:

- Name that you want assigned to the resource pool (required)
- Description of the resource pool (optional)
- Owner of the resource pool (optional)
- Contact e-mail address for anyone receiving alerts about the resource pool (optional)
- Time Zone used for actions involving the resource pool (optional to select a time zone other than the default)
- Physical Resources to associate with the resource pool (required)
- Resource Pool Label used for filtering resources during provisioning (optional)
- Space Thresholds for setting alerts for out-of-space conditions (optional to modify the default)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Resource Pools**.
2. Click **Add** to open the **Add Resource Pool** wizard and then complete the wizard.
3. Verify the creation and content of the resource pool by viewing the results that are displayed in the **Resource Pools** window.

## After you finish

You can use the **Datasets** window to associate the new resource pool with a new or existing dataset.

- If you want to associate a resource pool with a new dataset, use the **Add Dataset** wizard.
- If you want to associate a resource pool with an existing dataset, use the **Edit Dataset** window.

If you want to modify any of the properties of a resource pool, click **Edit** in the **Resource Pools** window.

## **Related concepts**

[\*Decisions to make before adding a resource pool\*](#) on page 837

[\*Effect of time zones on schedules\*](#) on page 1049

## **Related tasks**

[\*How do I back up data?\*](#) on page 589

## **Related references**

[\*Resource pool properties\*](#) on page 823

[\*Data ONTAP licenses used for protecting or provisioning data\*](#) on page 905

[\*Administrator roles and capabilities\*](#) on page 1055

[\*Resource pool guidelines\*](#) on page 831

# Impact of modifying resource pool properties

---

Before making changes to the properties of a resource pool, you need to understand the potential impact of those changes on your data protection setup.

Editing the Name, Description, Owner, or Contact properties for a resource pool does not impact the functioning of a resource pool; it only modifies the information viewed about the resource pool. However, editing the members or the time zone of a resource pool can have a significant impact on your data. The impact of modifying the membership of an existing resource pool depends on whether the resource pool is already associated with a dataset.

## Modifying a resource pool that is *not* associated with a dataset

Editing any of the properties of a resource pool that is not associated with a dataset does not impact any protected data. However, if you are modifying the resources or time zone of a resource pool, consider the potential result before making the change.

- Will the new size and number of aggregates be adequate for the intended use of the resource pool?
- Will a time zone change affect the schedule synchronization between the primary storage data and the secondary storage backup or mirror copy?

## Modifying a resource pool that *is* associated with a dataset

### Modifying the members of a resource pool

- Adding or removing the resources of a resource pool might affect the size and number of aggregates available for provisioning, once the resource pool is associated with a dataset.
- Removing resources: If an entire storage system is assigned to a resource pool, as aggregates are added to or removed from that storage system, the aggregates are automatically added to or removed from the resource pool that the storage system is associated with. You do not need to perform any additional tasks to have the aggregates available for provisioning.
- Adding resources: Verify that any resource you plan to add to a resource pool is online, properly configured, and licensed for the purpose you intend for it.

Adding a resource that is not available for provisioning can result in lack of conformance. For example, if an aggregate you plan to add is nearly full, the application cannot provision from that aggregate and jobs involving that aggregate will fail.

### Modifying the time zone of a resource pool

- Does not affect data that is already protected.

- Might affect whether the replication schedule on the primary dataset synchronizes as expected with the schedule on secondary or tertiary destination storage in the resource pool.

#### **Related concepts**

[\*Effect of time zones on schedules\*](#) on page 1049

#### **Related tasks**

[\*Editing resource pool properties\*](#) on page 845

# Editing resource pool properties

---

You can edit the properties of an existing resource pool by using the Edit properties option, accessible from the **Resource Pools** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. edit resource pool settings, such as the `GlobalFullControl` role.

Have the information available that you need to complete this task, depending on which properties you intend to edit:

- Settings
  - Name you want assigned to the resource pool
  - Description of the resource pool
  - Owner of the resource pool
  - Contact e-mail addresses for the people or aliases to alert regarding problems
  - Time Zone used for the resource pool
- Resources  
Be sure the resources you add to the resource pool have the proper configuration and licensing for their intended use.
- Labels to be associated with the resource pool or the aggregates
- Space Thresholds
  - Nearly full threshold
  - Full threshold
  - Nearly overcommitted threshold
  - Overcommitted threshold

## Steps

1. From the navigation pane, click **Data > Resource Pools**.
2. In the list of available resource pools, select the resource pool that you want to modify.
3. Click **Edit** to open the **Properties** sheet.
4. Modify the properties that you want changed.
5. Click **OK**.
6. Verify the changes to the resource pool properties.

You can verify the changes by viewing the information displayed in the **Resource Pools** window.

The resource pool's properties configuration is modified and saved.

### **After you finish**

Verify that any data set associated with the modified resource pool is still in conformance with any assigned provisioning or protection policies.

### **Related concepts**

*[Impact of modifying resource pool properties](#)* on page 843

### **Related references**

*[Resource pool properties](#)* on page 823

*[Administrator roles and capabilities](#)* on page 1055

*[Resource pool guidelines](#)* on page 831

# What a protection policy is

---

Protection policies define how protection relationships should be structured and the property settings for each component of the structure. If you also have the Disaster Recovery license, protection policies can also define how to fail over to secondary storage on the disaster recovery node when disaster occurs.

When a protection policy is applied to a dataset, it defines how data stored in dataset members should be backed up or mirrored. You can configure a protection policy that specifies a single protection method (local backup, remote backup, or mirroring) or a combination of those methods. For example, a protection policy might specify that the primary data is backed up to a secondary location and that the secondary copies are mirrored to a tertiary location.

If the Disaster Recovery license is installed, protection policies that use Qtree SnapMirror to back up data can also invoke your site's disaster recovery script. After the problem is resolved, you can move dataset member access manually from the secondary storage back to the primary storage.

## Related concepts

[\*Decisions to make before adding datasets\*](#) on page 711

[\*Dataset protection decisions\*](#) on page 711

[\*Decisions to make before assigning or changing policies\*](#) on page 721

[\*Types of data protection\*](#) on page 235

[\*Protection policy nodes and connections\*](#) on page 237

[\*Retention of hourly, daily, weekly, and monthly backups\*](#) on page 241

[\*Protection policy node prerequisites\*](#) on page 1051

[\*Allowable lag times\*](#) on page 247

[\*Protection schedules and time zones\*](#) on page 301

## Related tasks

[\*Assigning or changing a protection policy\*](#) on page 725

## Related references

[\*Protection policies \(not disaster recovery capable\)\*](#) on page 669



# Types of data protection

---

The protection policies provided by the licensed protection application enable you to select a combination of three types of data protection: local backup, remote backup, and mirror copy.

## Next topics

- [\*Local backup protection\* on page 235](#)
- [\*Remote backup protection\* on page 235](#)
- [\*Mirror protection\* on page 236](#)

## Related concepts

- [\*What a protection policy is\* on page 847](#)

## Local backup protection

Local backup protection (also referred to as Snapshot copy protection) is the periodic capture of active data on a NetApp storage system in backup images and the storage of those images on that same system.

If active data on the local system is accidentally deleted or corrupted, it can quickly be restored with the most recent image stored locally from the last local backup job.

Local backup operations are typically employed on the primary storage systems, where data is being actively updated and where, in event of accidental data loss, data restoration from the last hour or two might be required.

Local backup protection is based on Snapshot technology.

**Note:** Local backup protection is not available for datasets that include Open Systems SnapVault directories.

## Remote backup protection

Remote backup protection is the periodic capture and copying of active data from a source storage system to a remote secondary or tertiary storage system.

If data in the source storage system is lost and unrecoverable from its local backup (for example, if the source system is damaged) then data can still be restored quickly from the remote backup site.

Remote backup operations are employed from primary to secondary storage and from secondary to tertiary storage, in circumstances where secure storage of backup data at a remote site might be required.

If a disaster recovery license is installed, the licensed protection application enables you to supplement remote backup operations with additional failover instructions that transfer the primary storage function to a secondary storage site if disaster or mishap disables or destroys the original primary storage site.

Remote backup protection is based on SnapVault technology and Qtree SnapMirror technology.

## Mirror protection

Mirror protection is the periodic exact mirroring of all volume data (both active and protected) from a source storage system to a destination storage system.

If data in the source storage system is lost or made unavailable (for example if the source system is damaged) then that same data can quickly be made available from the destination mirror-copy site.

Mirror operations are employed from primary to secondary storage and from secondary to tertiary storage, in circumstances where secure mirroring of that data, and in event of breakdown at the source site, quick availability of that data from a second site might be required.

If a disaster recovery license is installed, the protection application enables you to supplement mirror operations with additional failover instructions that transfer the primary storage function to a secondary storage site if disaster or mishap disables or destroys the original primary storage site.

Mirror protection is based on Volume SnapMirror technology.

**Note:** Mirror operations that are scheduled and applied to a storage system through the licensed protection application replace and cancel any other SnapMirror operations or jobs that were configured locally on that storage system by other means. Backup operations that are scheduled and applied to a storage system through the licensed protection application run in addition to any other SnapVault operations that were configured locally on that node by other means.

# Protection policy nodes and connections

---

When you select a protection policy from the list on the **Protection Policies** window, the licensed protection application displays a diagram of that policy that represents its primary storage node, any backup node, any mirror node, and the backup or mirror connections between them.

In the diagram, the primary, backup, or mirror nodes are labeled either with default names, ("Primary Data," "Backup," or " Mirror") or user-assigned names if they have been assigned. You define the policy settings by clicking user-assigned or system-generated names and setting parameters for your protection policy's nodes and connections.

If you edit an existing policy, the protection application displays a list of the nodes and connection components that you can configure. You can modify one, two, or three nodes and zero, one, or two connections, depending upon the complexity of the protection policy and the methods of protection it employs.

**Primary data node** The protection policy *primary data node* is the component on which you specify local backup schedules, retention times, optional allowable local backup lag times, and optional DFPM-based backup scripts to be applied to the primary data location. Initially the protection application names this node "Primary data." You can specify another name.

**Note:** Local backup schedules and retention times do not apply to Open Systems SnapVault Windows, UNIX, or Linux-based primary storage systems.

**Backup connection** The protection policy *backup connection* is the component on which you specify remote backup schedules, optional throttle schedules, and optional allowable backup lag times if you are configuring a policy that uses remote backup protection. The protection application generates a name for this connection based on the names of the backup source and target nodes, for example: *Primary data to Backup*.

**Backup node** The protection policy *backup node* is the component on which you specify retention times for data backed up to a backup node. Initially the protection application names this node "Backup." You can specify another name.

**Mirror connection** The protection policy *mirror connection* is the component on which you specify mirroring schedules, optional throttle schedules, and optional allowable mirroring lag times. The protection application generates a name for this connection based on the names of the mirror-copy source and target nodes, for example: *Primary data to Mirror*.

**Mirror node** The protection policy *mirror node* is the component on which you can modify the name of the mirror-copy destination if you are configuring a policy that uses mirror-copy protection. Initially the protection application names this node "Mirror." You can specify another name.

**Related concepts**

*What a protection policy is* on page 847

# **Protection policies (not disaster recovery capable)**

Protection policies are the backup instructions that you assign to your datasets. These policies describe the type of backup to carry out, the Snapshot copy retention count, what preconfigured Snapshot copy, backup, and throttle schedule to follow, and what scripts to execute. The same policy can be assigned to multiple datasets.

The licensed protection application provides templates for you to configure the following types of backup setups:

**Note:** If the Disaster Recovery feature is licensed on your protection server, additional disaster recovery capable protection policies are available.

<b>Back up</b>	A dataset is backed up locally and also backed up from primary storage to secondary storage on a SnapVault or SnapMirror storage system.
<b>Back up, then Mirror</b>	A dataset is backed up from primary storage to secondary storage on a SnapVault or SnapMirror storage system and from there mirrored to a SnapMirror partner.
<b>Mirror then Mirror</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and from there mirrored to an additional SnapMirror partner.
<b>Local Snapshot copies only</b>	A dataset uses only local Snapshot copies in primary storage to protect data. No backup to secondary storage is implemented.
<b>Mirror</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner.
<b>Mirror and back up</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and is also backed up to secondary storage on a SnapVault or SnapMirror storage system.
<b>Mirror and mirror</b>	A dataset is mirrored from primary storage to secondary storage on two different SnapMirror partners
<b>Mirror then back up</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and from there backed up to tertiary storage on a SnapVault or SnapMirror storage system.
<b>No protection</b>	A dataset is left with no Snapshot copies, backups, or mirror-copy protection of any kind.
<b>Remote backup only</b>	Data on a storage system is backed up remotely to secondary storage on a SnapVault or SnapMirror storage system. The licensed application carries out no local backup on the primary storage. This is the protection policy to assign to third party systems with Open Systems SnapVault installed.

**Related concepts**

*What a protection policy is* on page 847

**Related references**

*Disaster recovery capable protection policies* on page 627

# Retention of hourly, daily, weekly, and monthly backups

---

You can schedule four classes of backup (hourly, daily, weekly, monthly) for retention purposes. When you assign a schedule to a protection policy, you can specify different minimum retention durations to preserve each category backup on your primary, secondary, or tertiary storage.

## Next topics

[Backup retention strategies](#) on page 241

[Backup retention classes](#) on page 242

## Related concepts

[What a protection policy is](#) on page 847

## Backup retention strategies

*Retention duration* is the minimum length of time that you want your backup copies to be preserved and protected from deletion in your primary, secondary, or tertiary storage.

You can only specify retention durations for backup copies, not mirror copies.

To guarantee preservation of the most recent successful backups, the licensed protection application always retains copies of at least the last two successful backups even if those copies are older than their specified minimum retention duration.

How long you decide to retain a particular backup depends on the original purpose of that backup.

- Local backups of data, for example, at the primary storage location, executed every hour for the purpose of ensuring quick restoration of recent data that was deleted or corrupted by accident, might not need to be retained beyond a 24-hour duration.
- A daily remote backup, on the other hand, of data to a secondary storage location, carried out after working hours to ensure its preservation, and if necessary, restoration to its state on this particular date, might require a retention duration of a week or a month or longer.

A usual practice is to schedule frequent local data backups with short retention durations at the primary storage source, and less frequent remote backups of that data with longer retention duration to the secondary storage location. Backups of data from secondary storage to tertiary storage are usually scheduled least frequently but are stored with the longest retention duration in the tertiary storage location.

## Backup retention classes

The licensed protection application allows you to configure a schedule with up to four classes of backups (hourly, daily, weekly, and monthly). For each class you can specify different minimum retention durations when you assign that schedule to your primary data storage or a backup connection.

**Hourly backups** Hourly backups are retained in the target storage for at least the duration that you specify for the Backup Retention Duration: Hourly parameter of the primary node or backup node of a protection policy.

Common retention durations for hourly backups are for short durations of a day or two if you are also maintaining daily, weekly, or monthly backups of this data for longer durations.

**Daily backups** Daily backups are retained in the target storage for at least the duration that you specify for the Backup Retention Duration: Daily parameter of the primary node or backup node of the policy.

Common retention durations for daily backups are from five days to several weeks.

**Weekly backups** Weekly backups are retained in the target storage for at least the duration that you specify for the Backup Retention Duration: Weekly parameter of the primary node or backup node of the policy.

Common retention durations for weekly backups are from one month to several months.

**Monthly backups** Monthly backups are retained in the target storage for at least the duration that you specify for the Backup Retention Duration: Monthly parameter of the primary node or backup node of the policy.

Common retention durations for monthly backups are from five months to several years.

# Protection policy node prerequisites

---

Before you attempt to implement a protection policy on your dataset nodes, ensure that the storage systems in the datasets or physical resource pools that make up that node meet the correct configuration and licensing requirements.

- Storage that is the source of a backup connection (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume, qtree, or OSSV directory if it is not an application dataset
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVault Data ONTAP Primary (for remote backup protection)
- Storage that is the source of a backup connection configured for nondisruptive LUN restore (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume or qtree
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requires both of the following:
    - Data ONTAP Primary
    - Data ONTAP 7.3 or later
- Storage that is the source of a disaster recovery capable backup connection (to a NetApp storage system )
  - Configuration requirements are all of the following:
    - Qtree, volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes)
    - Dataset not configured for non-disruptive LUN restore
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a backup connection (Open System)
  - Configuration requirements: Open Systems SnapVault directory

- Storage system licensing requirements: Open Systems SnapVault client
- Storage that is the destination of a backup connection (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume
    - Qtree
    - Storage system or aggregate containing volumes and qtrees
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVaultData ONTAP Secondary (for remote backup protection)  
If the source is Windows, Linux, or UNIX, then SnapVault Windows, SnapVault Linux, or SnapVault UNIX is also required.
- Storage that is the destination of a backup connection configured for nondisruptive LUN restore (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Qtree or volume
    - Storage system or aggregate containing volumes and qtrees. Provisioning policy type (SAN or NAS) matches primary provisioning policy type or does not export storage.
  - Storage system licensing requirements are all of the following:
    - SnapVault
    - Data ONTAP Secondary
    - Data ONTAP 7.3 or later
- Storage that is the destination of a disaster recovery capable backup connection (to a disaster recovery node)
  - Configuration requirements:  
Volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes). No qtree on same storage system as the primary qtree. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a mirror connection (not disaster recovery capable)
  - Configuration requirements are any of the following:
    - Volume

- Qtree
  - Storage system, or aggregate, containing one of the above
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a disaster recovery capable mirror connection
    - Configuration requirements are all of the following:
      - Volume (possibly containing qtrees), aggregate (possibly containing volumes), *or* an entire storage unit (possibly containing aggregates or volumes)
      - Nothing that is in another dataset
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a mirror connection (not disaster recovery capable)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a disaster recovery capable mirror connection (to a disaster recovery node)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees. No volume on the same storage system as the primary volume. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
    - Storage system licensing requirements: SnapMirror
  - Any node
    - Configuration requirements: Nothing that is in a resource pool used by this dataset
    - Storage system licensing requirements: None
  - Primary (root) node with local backup schedule
    - Configuration requirements: No Open Systems SnapVault directories or Open Systems SnapVault hosts included
    - Storage system licensing requirements: None

- Non-root node
  - Configuration requirements: No Open Systems SnapVault directories or hosts and nothing that is in a non-root node of any other dataset and nothing that is in any node of this dataset.
  - Storage system licensing requirements: None

**Note:**

- If you plan to use SnapMirror with the licensed protection application, you must update the snapmirror.access option in Data ONTAP to specify the destination systems that are allowed to access the primary data source system.  
The snapmirror.access option specifies which SnapMirror destination systems can initiate transfers and which network interfaces they can use. For security reasons, the protection application does not modify the snapmirror.access option for you.
- A single storage system licensed as both SnapVault primary storage and SnapVault secondary storage locations cannot be included in a dataset.
- If you are restoring a LUN, the following points apply:
  - If the protection application is not configured to support non-disruptive LUN restore, the LUN in the destination location must be offline before you start the restore operation.
  - If the protection application is configured to support non-disruptive LUN restore, the LUN in the destination does not have to be offline unless it is owned by a vFiler unit.
  - If the destination LUN is owned by a vFiler unit, non-disruptive LUN restore is not supported.

**Related concepts**

[\*Decisions to make before adding datasets\*](#) on page 711

[\*Decisions to make before adding a resource pool\*](#) on page 837

[\*What a protection policy is\*](#) on page 847

# Allowable lag times

---

The lag time settings in a protection policy specify acceptable differences between the current time on a source node's system clock and the timestamp of the last successful backup or mirror copy of source data on the target node.

You can configure the licensed protection application to issue warning or error messages if the lag between the current time on a source node's system clock and the timestamp of the last successful backup or mirror operation to the target node differ enough to indicate failed or successively failed data protection operations.

- When the lag settings are applied to the primary node component of a protection policy  
The lag settings instruct the protection application to issue warning or error messages if successive local backup operations fail to the point that the time difference between the timestamp on the last successful local backup and the current time on the primary node system clock exceeds a user-specified threshold.  
On primary data nodes, warning or error messages related to lag settings might indicate that the local backup instructions, often transmitted from a controlling node, did not get sent, read, or executed.
- When the lag settings are applied to the backup connection or the mirror connection component of a protection policy  
The lag settings instruct the protection application to issue warning or error messages if successive remote backup or mirror operations fail to the extent that the time difference between the timestamp on the last successful remote backup or mirror copy and the current time on the target node system clock exceed a user-specified time period.  
On backup or mirror nodes, warning or error messages related to lag settings might indicate that transmission speeds between the source and target nodes are too slow to allow remote backup or mirror operations to successfully finish within their scheduled times.

## Related concepts

[What a protection policy is](#) on page 847



# Protection schedules and time zones

---

If the DataFabric Manager server that hosts the licensed protection application is located in a time zone different from the primary data node, backup node, or mirror node, the difference in time zone settings for the dataset or physical resource pool elements of those nodes might affect the execution of the protection or throttle schedules that you assign in your protection policy.

If a policy node's dataset or physical resource pool elements are not assigned a time zone setting, then by default the licensed protection application executes the protection schedule for that node or its backup or mirror connection in accordance with the clock and time zone setting on the DataFabric Manager server.

For example, without time zone settings on the primary data node datasets, a daily backup scheduled for 9 p.m. (Eastern Standard Time) from a protection application console and a DataFabric Manager server in New York will, by default, execute at 6 p.m. (Pacific Standard Time) on a primary data node in Los Angeles, or at 2 a.m. (GMT) at a primary data node in London.

However, if those Los Angeles and London datasets are assigned Pacific Standard Time and GMT time zone settings respectively, then the protection application adjusts the schedule to execute daily backups at 9 p.m. (Pacific Standard Time) in Los Angeles and at 9 p.m. (GMT) in London.

## Related concepts

[What a protection policy is](#) on page 847

[Effect of time zones on schedules](#) on page 1049



# **Decisions to make before adding a protection policy**

---

Before you use the **Add Protection Policy** wizard to add a new policy, you must make some decisions about the policy, node component, and connection component configuration information that you need to input for the wizard.

- [\*Protection policy decisions\*](#) on page 251
- [\*Primary node decisions\*](#) on page 251
- [\*Backup or mirror connection decisions\*](#) on page 252
- [\*Backup or mirror node decisions\*](#) on page 253

## **Protection policy decisions**

**Policy name and description** What name do you want to assign to the policy? What is the description for this new policy?

**Base policy operation** What base configuration do you want to use for the new policy (for example: Backup, or Backup then mirror, Local backup only, or Disaster Recovery Backup)?

- The licensed protection application provides 10 base combinations of data protection operations for you to select from.
- If a disaster recovery license is installed, the protection application provides an additional six disaster recovery-capable base protection policies.

## **Primary node decisions**

**Node name** What name do you want to assign to the primary storage node?

**Local backup schedule (for local backup of primary storage)** What is the optional schedule to apply if you want to implement local backup of data on the primary storage node?  
This schedule applies to local backup operations on primary data storage only.

**Backup retention durations (for local backup of primary storage)** Do you want to perform local backups of primary storage data?

If so, what is the minimum length of time (in hours, days, or weeks) you want to retain your scheduled hourly, daily, weekly, or monthly local backup copies on this primary storage node before they are deleted? These settings apply only to local backups in primary data storage.

<b>Backup script</b>	<p>Do you want to run an optional user-defined protection (<i>dfpm</i>) backup script on the DataFabric Manager server?</p> <p>If so, what are the parameters needed to run the script? Backup scripts can invoke preprocesses and postprocesses for backup or mirror operations (for example, quiescing data application activity on protection policy nodes prior to remote backup operation and restarting application activity after backup finishes).</p>
<b>Failover script (for disaster-recovery capable protection policies)</b>	<p>If you are providing disaster-recovery protection, do you want to use an optional user-defined protection (<i>dfpm</i>) failover script?</p> <p>Failover scripts can invoke processes to take place before and after the failover mirror relationship break if those processes are necessary. If you provide a failover script, what is its name and path location in relation to the DataFabric Manager server? What are the parameters needed to run the script?</p> <p><b>Note:</b> If the DataFabric Manager server is running on Windows, and if the failover script is located on a network share, the failover script location must be specified by the full UNC path (no drive mapping).</p>
<b>Lag</b>	<p>What is the maximum acceptable lag between the current time at the primary node and the timestamp of the last successfully completed local backup? Lags that exceed the specified period trigger either warning or error messages.</p> <ul style="list-style-type: none"><li><b>Warning threshold:</b> What is the number of minutes, hours, days, or weeks of lag that triggers a warning? Decide on a number that specifies a lag time that might cause concern. For example, if you follow a schedule that attempts a local backup operation every hour, specifying a two-hour Warning Threshold triggers a warning message in the event of two successive local backup failures.</li><li><b>Error threshold:</b> What is the number of minutes, hours, days, or weeks of lag that triggers an error message? Decide on a number that specifies an acceptable lag time that might cause concern. For example, if you follow a schedule that attempts a local backup operation every hour, specifying a three-hour Error Threshold triggers an error message in the event of three successive backup transfer failures.</li></ul> <p><b>Note:</b> If you specify an Error Threshold shorter than the Warning Threshold, the protection application disables lag-related warning messages.</p>

## Backup or mirror connection decisions

<b>Backup schedule</b>	What is the daily, weekly, or monthly schedule that you want applied to your backup operations to secondary or tertiary storage?
------------------------	--

<b>Mirror schedule</b>	What is the daily, weekly, or monthly schedule that you want applied to your mirror operations to secondary or tertiary storage?
<b>Throttle</b>	What is the bandwidth throttle schedule that you want to apply to your backup or mirror connections to secondary or tertiary storage?
<b>Lag</b>	<p>What is the maximum acceptable lag between the current time at a backup or mirror source node and the timestamp of the last successfully completed backup or mirror copy on the target node? Lags that exceed the specified period trigger either warning or error messages.</p> <ul style="list-style-type: none"> <li>• <b>Warning threshold:</b> What is the number of minutes, hours, days, or weeks of lag between backup data being sent and successfully backed up or mirrored at the target that triggers a warning?</li> </ul> <p>Decide on a number that specifies a lag time that might cause concern. For example, if you follow a schedule that attempts a backup or mirror operation every hour, specifying a two-hour Warning Threshold triggers a warning message in the event of two successive backup or mirror transfer failures.</p> <ul style="list-style-type: none"> <li>• <b>Error threshold:</b> What is the number of minutes, hours, days, or weeks of lag between backup data being sent and successfully backed up or mirrored at the target that triggers an error message?</li> </ul> <p>Decide on a number that specifies an acceptable lag time that might cause concern. For example, if you follow a schedule that attempts a backup or mirror operation every hour, specifying a three-hour Error Threshold triggers an error message in the event of three successive backup transfer failures.</p> <p><b>Note:</b> If you specify an Error Threshold shorter than the Warning Threshold, the protection application disables lag-related warning messages.</p>

## Backup or mirror node decisions

<b>Node Name</b>	What name do you want to assign to the secondary or tertiary backup or mirror node?
<b>Backup retention duration</b>	If your policy includes backups to secondary or tertiary storage, what is the minimum length of time (in minutes, hours, days, or weeks) you want to retain scheduled hourly, daily, weekly, or monthly backups on a secondary or tertiary storage node before they are deleted?

## Related concepts

[Effect of time zones on schedules](#) on page 1049

## Related tasks

[Adding a daily protection schedule](#) on page 307

[Adding a weekly protection schedule](#) on page 309

*Adding a monthly protection schedule* on page 311

*Adding a throttle schedule* on page 313

*Adding a protection policy* on page 671

*How do I back up data?* on page 589

# Adding a protection policy

---

You can use the **Add Protection Policy** wizard to create new protection policies. After you create a protection policy, you can apply it to datasets to manage the backup or mirror operations that are executed on those datasets.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the information available that you need to complete this task:

- Policy name, base configuration, name for each node
- Primary node information
- Backup or mirror connection information:
- Backup or mirror node information:

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Click **Add** to start the **Add Protection Policy** wizard.
3. Type a policy name and description and click **Next**.
4. Select a base policy and click **Next**.
5. Complete the policy property sheets for the primary node and any backup connection, mirror connection, secondary storage, or tertiary storage node that is required for the policy. After you complete each property sheet, click **Next**.

After all property sheets are completed, the **Add Protection Policy** wizard displays a summary sheet for the policy.

6. Confirm the details of the policy and click **Finish**.

Your new policy is listed on the **Protection Policies** window Overview tab.

## Related concepts

*Decisions to make before adding a protection policy* on page 251

## Related tasks

*Enabling disaster recovery protection* on page 641

## Related references

*Administrator roles and capabilities* on page 1055



# Editing a protection policy

---

You can edit a protection policy by selecting it in the **Protection Policies** window and clicking the Edit button.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy you want to modify.

The licensed protection application displays a diagram showing the primary node, backup node, or mirror node components that are included in the selected policy. By default the node types are labeled Primary Data, Backup, and Mirror, but they might also be labeled with alternative user-assigned names.

### Note:

- If the primary, backup, or mirror nodes have user-assigned names rather than their default Primary Data, Backup, or Mirror labels, note the user-assigned names.
- As a shortcut, you can directly display and edit the properties of any policy node or connection component by clicking it in the diagram.

3. If the diagram notes that dependencies exist for the selected policy, click the **Dependencies** tab to ensure that you apply the policy edits to the all the datasets in the Dependencies list.
4. Click **Edit**.
5. In the **Properties** sheet, click **Nodes and Connections** and note the selectable node and connection names that are displayed in the list.

A policy's backup connection or mirror connection components are listed by labels that are generated from the names of the source and target nodes: for example, "Primary to Backup" or "Primary to Mirror."

6. Click each node or connection in the list to display and edit the properties for that component.
7. After you complete your modifications, click **Preview**.
8. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.

- Click **OK** to apply your changes and close the **Properties** sheet.

## Next topics

- [Editing a policy's primary data node](#) on page 258
- [Editing a policy's backup connection](#) on page 259
- [Editing a policy's backup node](#) on page 260
- [Editing a policy's mirror connection](#) on page 260
- [Editing a policy's mirror node](#) on page 261

# Editing a policy's primary data node

You can edit the local backup schedule, backup script, allowable lag, retention durations, and node name specifications on a policy's primary data node.

## Before you begin

- Have the policy information available that you need to complete its primary node specifications:
  - Node name
  - Local backup schedule
  - Backup retention duration (of the local backup)
  - Backup script (if any)
  - Failover script (if the policy is disaster recovery capable)
  - Lag warning thresholds and Lag error thresholds
- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance..

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the primary data node you want to modify and click **Edit > Nodes and Connections**.
3. Select the primary node.

The node is named either "Primary node" or the user-assigned name for that node.

The primary data node properties are displayed in the properties area.

4. Modify the primary node properties, as needed, and click **Preview**.

5. Review the effects of your changes and do one of the following:

- Click **Apply** to apply your changes and continue to edit the current policy.
- Click **OK** to apply your changes and close the **Properties** sheet.

**Related references**

[Administrator roles and capabilities](#) on page 1055

## Editing a policy's backup connection

You can edit the backup schedule, throttle schedule, and lag allowance specifications on the backup connection of a protection policy.

**Before you begin**

- Have the policy information available that you need to complete its backup connection specifications:
  - Backup schedule
  - Throttle schedule
  - Lag warning thresholds and Lag error thresholds
- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Steps**

1. From the navigation pane, click **Policies** ▶ **Protection** ▶ **Overview**.
2. Select the protection policy that has the backup connection you want to modify and click **Edit** ▶ **Nodes and Connections**.
3. Select the backup connection.
4. Modify the backup connection properties, as needed, and click **Preview**.
5. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

**Related references**

[Administrator roles and capabilities](#) on page 1055

## Editing a policy's backup node

You can edit the hourly, daily, weekly, or monthly backup retention durations on the backup node of a protection policy.

### Before you begin

- Have the policy information available that you need to complete its backup node specifications:
  - Node name
  - Backup retention duration (of the backups to the backup node)
- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the backup node you want to modify and click **Edit > Nodes and Connections**.
3. Select either "Backup" or the user-assigned name for that node.
4. Modify the backup node properties, as needed, and click **Preview**.
5. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

### Related references

[Administrator roles and capabilities](#) on page 1055

## Editing a policy's mirror connection

You can edit protection schedule, throttle schedule, and allowable lag specifications on a protection policy's mirror connection.

### Before you begin

- Have the policy information available that you need to complete its mirror connection specifications:

- Mirror schedule
- Throttle schedule
- Lag warning thresholds and Lag error thresholds
- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the mirror connection you want to modify and click **Edit > Nodes and Connections**.
3. Select the mirror connection.
4. Modify the backup node properties, as needed, and click **Preview**.
5. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

## Related references

[Administrator roles and capabilities](#) on page 1055

# Editing a policy's mirror node

You can edit the name the backup node of a protection policy.

## Before you begin

- Have the policy information available that you need to the mirror node name.
- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the mirror node you want to modify and click **Edit > Nodes and Connections**.

3. Select either **Mirror** or the user-assigned name for that node.
4. Modify the mirror node properties, as needed, and click **Preview**.
5. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

#### **Related references**

*[Administrator roles and capabilities](#)* on page 1055

# Assigning or changing schedules in a protection policy

---

You can assign or change protection and throttle schedules for the primary node, backup connection, or mirror connection of a protection policy.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Confirm that time zone differences and settings on the DataFabric Manager server, and the dataset or physical resource pool elements of the policy nodes support the new schedule assignment.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the local backup, remote backup, or mirror schedule assignment you want to modify and click **Edit > Nodes and Connections**.
3. Select the primary node, backup connection, or mirror connection that you want to modify.
4. Locate the appropriate schedule in the Properties area (Local Backup Schedule, Backup Schedule Name, Mirror Schedule Name, or Throttle Schedule Name) and select a new schedule from the schedule drop-down list.
5. After you complete your modifications, click **Preview**.
6. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

The modifications take effect immediately.

## Related tasks

[How do I back up data?](#) on page 589

## Related references

[Administrator roles and capabilities](#) on page 1055



# Changing retention times in a protection policy

---

You can vary and modify the minimum duration that the scheduled backup copies of your protected data are retained on the target nodes before they are deleted.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Make sure that the resource pools for the secondary storage contain sufficient capacity to support the retention durations that you want to specify.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the primary or backup node on which you want to assign or modify the retention times and click **Edit > Nodes & Connections**.
3. In the Nodes and Connections list, select the primary or backup node on which you want to assign or modify the retention times.
4. Locate the retention duration (Hourly, Daily, Weekly, or Monthly) in the Properties area and assign or modify the values.
5. After you complete your modifications, click **Preview**.
6. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

The modifications take effect immediately.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Changing lag thresholds in a protection policy

---

You can modify the lag time allowed between transmission of protected data from a backup or mirror source node to its successful reduplication at a target node. Lag times that exceed your specifications trigger either a warning or an error message for the backup or mirror operation during which they occur.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the primary node, backup connection, or mirror connection on which you want to modify the lag times and click **Edit > Nodes & Connections**.
3. In the Nodes and Connections list, select the primary node, backup connection, or mirror connection you want to modify.
4. Specify the new lag times.
5. After you complete your modifications, click **Preview**.
6. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

The modifications take effect immediately.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Changing a node name in a policy

---

You can edit the name that labels the primary data node, backup node, or mirror node object in a protection policy diagram.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy. If it is not, then you might want to add a new protection policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the primary, backup, or mirror node that you want to modify and click **Edit > Nodes & Connections**.
3. In the Nodes and Connections list, select the primary, backup, or mirror node that you want to modify.
4. In the Node Name parameter, specify the new name for that node.
5. After you complete your modifications, click **Preview**.
6. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

The modifications take effect immediately.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a protection policy

---

You can delete an existing protection policy if that policy is not currently applied to any existing dataset.

## Before you begin

- You can use the Dependencies tab to confirm that the protection policy that you want to delete is no longer assigned to any existing datasets.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. In the Policies list box, select the protection policy that you want to delete.
3. Click **Delete**, then click **Yes** on the confirmation prompt.

The Delete button is not enabled for policies still attached to datasets.

The selected protection policy is deleted from the protection policies list.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Effect of time zones on schedules

---

Understanding how time zone settings can affect your protection schedules is important to be sure your backups and mirror copies are functioning as intended.

In Protection Manager, you determine the time zone to be used for a protection schedule when you set up your resource pools and your datasets. You have a choice of using the DataFabric Manager server's default time zone, creating a new default for datasets and resource pools, or selecting a different time zone each time you create or edit a dataset or resource pool in Protection Manager. The dataset contains your primary data and the resource pool contains destination storage that is available for provisioning to hold backups and mirror copies of your data.

Before selecting a schedule for a replication job, you need to know the time zones associated with the primary data and destination storage for that job. That information helps you determine when you want your local backups to occur, and when you want the remote replication to take place to achieve your data protection goals.

When the licensed protection application interprets a scheduled replication from primary data in a dataset to secondary destination storage, it uses the time zone of the primary data. When interpreting a scheduled replication from secondary storage to tertiary storage, the licensed protection application uses the time zone of the secondary node.

If you misapply time zones, unexpected and unwanted results could occur. For example, a weekly mirror copy to tertiary storage might occur before completion of the daily backup that you want to capture, or replication jobs might occur at a time of day when network bandwidth is already servicing a heavy load, and so forth.

**Note:** Some time zones observe daylight saving time (DST) and some do not. The licensed protection application automatically observes the local time zone and adjusts for daylight saving when appropriate. As a result, backups scheduled during the DST transition, between 1:00 am and 3:00 am local time, might not perform as intended.

## Next topics

[Ways to set the time zone](#) on page 274

[Guidelines for using time zones with resource pools](#) on page 276

[Guidelines for using time zones with datasets](#) on page 277

## Related concepts

[Decisions to make before adding datasets](#) on page 711

[Decisions to make before adding a resource pool](#) on page 837

[Impact of modifying resource pool properties](#) on page 843

[Dataset protection decisions](#) on page 711

[Protection schedules and time zones](#) on page 301

[Decisions to make before adding a protection policy](#) on page 251

[Planning schedules for protection policy nodes and connections](#) on page 293

[Protection schedules and time zones](#) on page 301

## Related tasks

[Adding a dataset](#) on page 719

[Adding a resource pool](#) on page 841

## Related references

[Example of a schedule using local time zones](#) on page 279

[Example of a schedule using a default time zone](#) on page 283

## Ways to set the time zone

There are three ways you can set the time zone you want the licensed protection application to use when interpreting schedules for dataset replication jobs: use the DataFabric Manager server's system default time zone, set a new default time zone, or use the licensed protection application to set the time zone.

- **Operations Manager system default**

By default, the licensed protection application uses the DataFabric Manager server's system time zone setting when interpreting the times and dates in a protection schedule. The system time can be viewed in the DataFabric Manager user interface.

You might use the server's system time zone if your primary data and the server are both in the same time zone.

- **DataFabric Manager timezone option**

You can change the default time zone available for datasets and resource pools. Use the command `dfm option set timezone=timezone` on the DataFabric Manager server's command line to specify the new default.

If this global time zone value is left empty, the original system default time zone is used. If the global time zone value is set by using `dfm option set timezone`, that value becomes the new

default time zone for datasets and resource pools. You can use the `dfm option list timezone` command to display the current system default time zone, if one is set.

You might set a new default with the `timezone` option if most of your primary data is collocated in a single time zone, but in a different time zone than the server.

**Note:** Setting a new default by using the `timezone` option only affects the default time zone for datasets and resource pools. It does not impact the DataFabric Manager server's system default time zone setting. More information about this command option is available in the related man page in the online Help.

- **Protection Manager interface**

You can override the original or the modified default Time Zone setting by using the time zone selection lists when you add or modify a dataset or resource pool.

The protection dataset and resource pool time zone lists provide options for how you can display the time zone you want to use. You might want to have each time zone identified by the city in which the data is located; or perhaps you prefer to use the official abbreviation for a time zone. Some examples of the choices offered in the time zone lists include the following:

<b>Region/City</b>	Example: Europe/Istanbul Example: America/Montreal
<b>City or Country</b>	Example: Turkey Example: Canada/Eastern
<b>Time zone abbreviation</b>	Example: EET (Eastern European Time) Example: EST5EDT (Eastern Standard Time/Eastern Daylight Time)

The selected time zone appears highlighted in the time zone list, whether it's a default value or a user-selected value.

You might use the protection application to override the server's time zone if:

- Most of your data is spread out across a number of different time zones.
- You want a replication job for a particular dataset or a particular resource pool to occur in a time zone other than the default.

## Related references

[Example of a schedule using local time zones](#) on page 279

[Example of a schedule using a default time zone](#) on page 283

## Guidelines for using time zones with resource pools

When creating or editing a resource pool, you can select a time zone to associate with the resource pool. Review these guidelines to help you determine whether to use the default time zone, or select a new one, for your resource pool.

- In the licensed protection application, you can select a time zone other than the default for any resource pool, but you do not have to.  
You select a time zone for an individual resource pool from the **Resource Pools** window. Click the Add button to access the **Add Resource Pool** wizard, or click the Edit button to open the **Properties** sheet.
- If you do not select a time zone, the licensed protection application uses either the DataFabric Manager server's system default value, or the default value set with the `dfm option set timezone=<timezone>`, as described under "Ways to Set the Time Zone".
- When you assign a time zone to a resource pool, any policy node associated with that resource pool will use the resource pool's time zone.
- When you set a time zone for a resource pool in the protection application interface, the time zone applies only to the data on the secondary destination node. It does not impact the primary data in a dataset. Different time zones can be selected for replication of primary data to a secondary resource and for the replication of data from a secondary to a tertiary resource.
- For two-node policies, the protection application uses the time zone of the primary data to interpret schedules for data transfers.

This is true even if a resource pool is associated with the dataset, and that resource pool has a time zone assigned to it that is different from the dataset's time zone.

- You might want to change the default time zone for a resource pool when working with a three-node policy.

If you want data transfers from the second node to the third node to be scheduled in the "local time" of the second node, you specify a time zone for the resource pool that contains the second node.

- If you change the default time zone by using the `dfm option set timezone=<timezone>` command, then all resource pools that use that default setting begin using the new default value. Be sure any changes to the time zone are thoroughly evaluated for potential impact to schedules, as changes could disrupt the intended schedules for future jobs.

Datasets and resource pools for which the time zone is set by using the protection application user interface will not be affected by changes made using the `timezone` option. This is because the licensed protection application setting overrides any default setting.

### Related references

[Example of a schedule using local time zones](#) on page 279

[Example of a schedule using a default time zone](#) on page 283

## Guidelines for using time zones with datasets

When creating or editing a dataset, you can select a time zone to associate with the dataset. Review these guidelines to help you determine whether to use the default time zone, or select a new one for your dataset.

- You can select a time zone other than the default for any dataset, but you do not have to. You select a time zone for an individual dataset from the **Datasets** window. Click **Add** to access the **Add Dataset** wizard, or click **Edit**, to open the **Properties** sheet.
- If you do not select a time zone, the licensed protection application uses either the DataFabric Manager server's system default value, or the default value set with the `dfm option set timezone=<timezone>`, as described under "Ways to Set the Time Zone".
- If you associate a time zone with a dataset, the protection application uses the time zone you selected, rather than the server's system default, to interpret schedules affecting data in that dataset.
- When you set a time zone for a dataset in the protection application interface, the time zone applies only to the primary data in the dataset. It does not impact any destination nodes or resource pools.
- The start and end time of a local or a remote replication is determined by the time zone selected for the primary data in the dataset. The time zone selected for any resource pool associated with the dataset does not impact the time of the replication event starting on the primary.
- When you might want to change the default time zone:
  - If most of the primary data is in a different time zone than the DataFabric Manager server, you might want to set the DataFabric Manager global command, `dfm option set timezone=<timezone>`, to specify which time zone the licensed protection application should use for interpreting all schedules.
  - If most of your datasets are distributed across different time zones, and you want the schedules interpreted in the "local time" for each dataset, you specify each dataset's time zone in the licensed protection application user interface.

### Related references

[Example of a schedule using local time zones](#) on page 279

[Example of a schedule using a default time zone](#) on page 283



# Example of a schedule using local time zones

---

This example describes the setup and results of selecting local time zones for the dataset and resource pools, rather than using the server's system default.

There are three parts to this example.

1. [Time zone assignment \(local\)](#) on page 279
2. [Time zone selection for protection schedules \(local\)](#) on page 280
3. [Results of scheduled jobs \(local\)](#) on page 281

## Related concepts

[Effect of time zones on schedules](#) on page 1049

[Ways to set the time zone](#) on page 274

[Guidelines for using time zones with datasets](#) on page 277

[Guidelines for using time zones with resource pools](#) on page 276

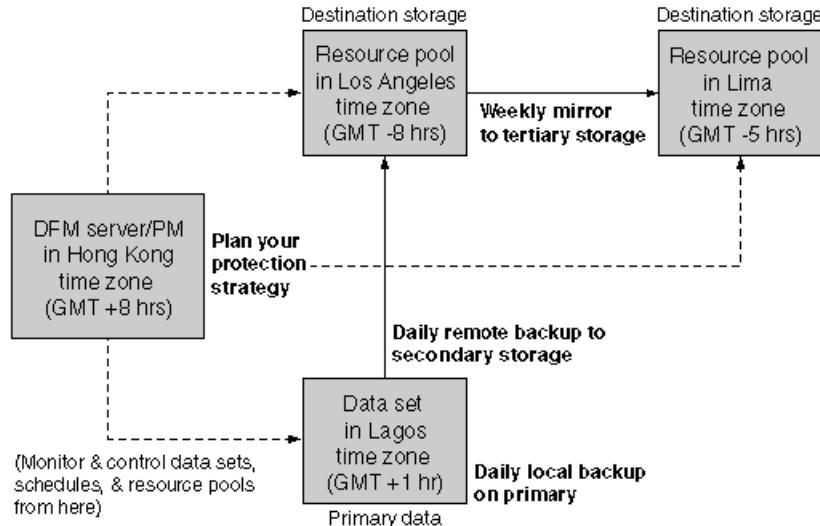
## Time zone assignment (local)

This example shows how the administrator sets up a local time zone for the server, dataset, and destination storage.

Assume the following:

- A DataFabric Manager server is located in Hong Kong, China.  
The administrator selected the Hong Kong time zone (GMT +8 hrs.) for the server.  
From this server in the Hong Kong time zone, the administrator used Protection Manager to create the resource pools, datasets, and protection schedules.
- A dataset containing primary data is located in Lagos, Nigeria.  
The administrator selected the Africa/Lagos time zone (GMT +1 hr.) for the dataset.  
The administrator overrode the server's default time zone with the Lagos time zone when creating the dataset that contains the primary data. Therefore, Protection Manager interprets the times and dates of the protection schedule in the Lagos time zone.
- Resource pools provisioned as backup destination storage are located in the city of Los Angeles in the United States.  
The administrator selected the PST8PDT time zone (GMT -8 hrs.) for the resource pool.  
The administrator overrode the server's default time zone with the PST8PDT time zone when creating the resource pool for the secondary destination storage. Therefore, Protection Manager interprets the times and dates of the protection schedule in Los Angeles time for replicating data from the secondary storage to the tertiary storage.

- Resource pools provisioned as tertiary destination storage for mirroring are located in Lima, Peru. The administrator selected the America/Lima time zone (GMT -5 hrs.) for the tertiary storage. The administrator overrode the server's default time zone with the Lima time zone when creating the resource pool for the tertiary destination storage.



## Time zone selection for protection schedules (local)

This example shows how the administrator selects the local time zone for the protection schedules.

From the DataFabric Manager server in the Hong Kong time zone, you schedule the following:

- A Daily local backup of the primary data at 8:00 p.m. Monday  
8 p.m. Hong Kong = 1:00 p.m. Lagos = 4:00 a.m. Los Angeles = 7:00 a.m. Lima
- A Daily remote backup of the primary data in Nigeria to secondary storage in the U.S. at 11:00 p.m. Monday  
11 p.m. Hong Kong = 4:00 p.m. Lagos = 7:00 a.m. Los Angeles = 10:00 a.m. Lima
- A Weekly mirror copy of the secondary storage from the U.S. to tertiary destination storage in Peru at 6:30 p.m. Monday

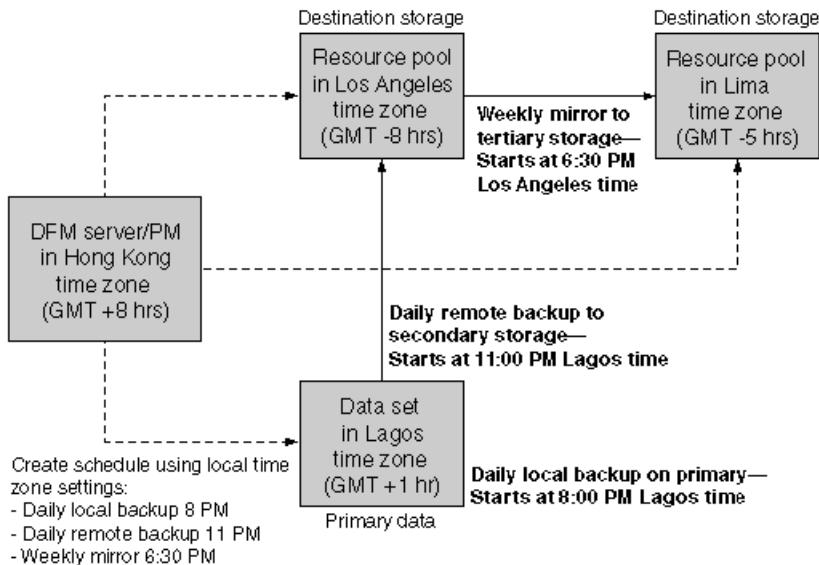
## Results of scheduled jobs (local)

This example shows the results of protection jobs using the local time zone for the protection schedules.

The following actions occur, assuming that the replication jobs all succeed:

- Protection Manager interprets the Daily local backup schedule in the time zone of the primary data, therefore, the backup starts at 8:00 p.m. Monday, Lagos time.
- Protection Manager interprets the Daily remote backup schedule in the time zone of the primary data, therefore, the remote backup starts at 11:00 p.m. Monday, Lagos time. Protection Manager starts the backup, replicating primary data in Nigeria to backup destination storage in Los Angeles.
- Protection Manager interprets the Weekly mirror schedule in the time zone of the secondary storage, therefore, remote mirroring starts at 6:30 a.m. Monday, Los Angeles time. Protection Manager mirrors the data, replicating the backed-up data on the secondary storage in the U.S. to tertiary storage in Lima.

The location and time zone of the tertiary destination storage does not impact the schedule.





## **Example of a schedule using a default time zone**

---

This example describes the set up and results of selecting the DataFabric Manager server's default time zone for the dataset and resource pool associated with a protection schedule.

There are three parts to this example.

1. [\*Time zone assignment \(default\)\*](#) on page 283
2. [\*Time zone selection for protection schedules \(default\)\*](#) on page 284
3. [\*Results of scheduled jobs \(default\)\*](#) on page 285

### **Related concepts**

[\*Effect of time zones on schedules\*](#) on page 1049

[\*Ways to set the time zone\*](#) on page 274

[\*Guidelines for using time zones with datasets\*](#) on page 277

[\*Guidelines for using time zones with resource pools\*](#) on page 276

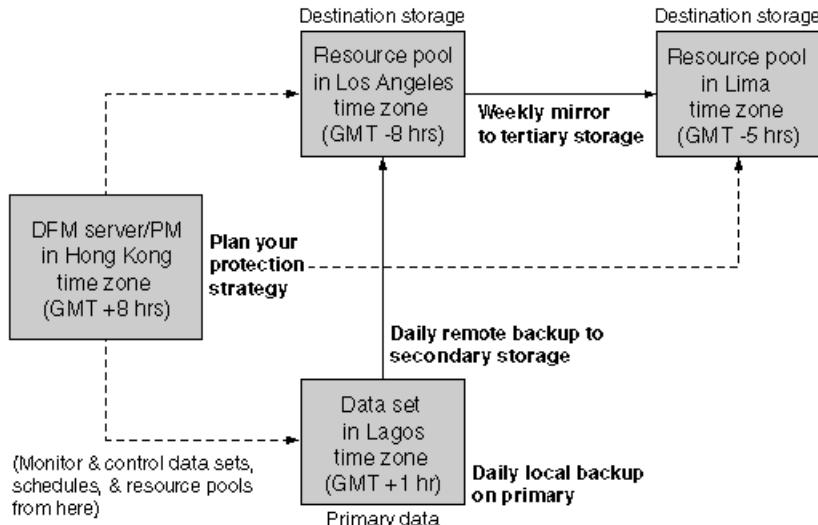
## **Time zone assignment (default)**

This example shows how the administrator sets up a default time zone for the server, dataset, and destination storage.

Assume the following:

- An DataFabric Manager server is located in Hong Kong, China.  
The administrator selected the Hongkong time zone (GMT +8 hrs.) for the server.  
From this server in the Hong Kong time zone, the administrator used Protection Manager to create the resource pools, datasets, and protection schedules.
- A dataset containing primary data is located in Lagos, Nigeria.  
The administrator selected the Africa/Lagos time zone (GMT +1 hr.) for the dataset.  
The administrator selected the server's default time zone when creating the dataset that contains the primary data. Therefore, Protection Manager interprets the times and dates of the protection schedule in the Hongkong time zone.
- Resource pools provisioned as backup destination storage are located in the city of Los Angeles in the United States.  
The administrator selected the PST8PDT time zone (GMT -8 hrs.) for the resource pool.  
The administrator selected the server's default time zone when creating the resource pool for the secondary destination storage. Therefore, Protection Manager interprets the times and dates of the protection schedule in the Hongkong time zone for replicating data from the secondary storage to the tertiary storage .

- Resource pools provisioned as tertiary destination storage for mirroring are located in Lima, Peru. The administrator selected the America/Lima time zone (GMT -5 hrs.) for the tertiary storage. The administrator selected the server's default time zone when creating the resource pool for the tertiary destination storage.



## Time zone selection for protection schedules (default)

This example shows how the administrator selects the default time zone for the protection schedules.

From the DataFabric Manager server in the Hong Kong time zone, you schedule the following:

- A Daily local backup of the primary data at 8:00 p.m. Monday  
8 p.m. Hong Kong = 1:00 p.m. Lagos = 4:00 a.m. Los Angeles = 7:00 a.m. Lima
- A Daily remote backup of the primary data in Nigeria to secondary storage in the U.S. at 11:00 p.m. Monday  
11 p.m. Hong Kong = 4:00 p.m. Lagos = 7:00 a.m. Los Angeles = 10:00 a.m. Lima
- A Weekly mirror copy of the secondary storage from the U.S. to tertiary destination storage in Peru at 6:30 p.m. Monday

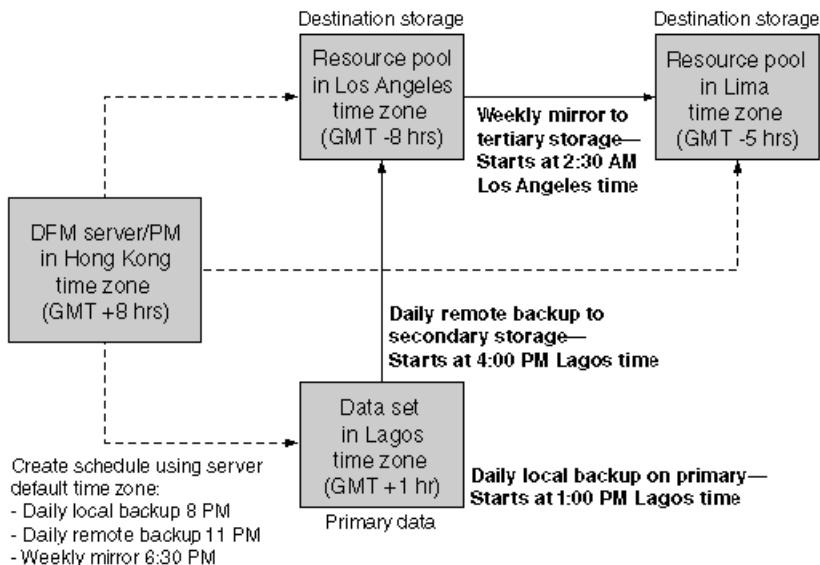
## Results of scheduled jobs (default)

This example shows the results of protection jobs using the default time zone for the protection schedules.

The following actions occur, assuming the replication jobs all succeed:

- Protection Manager interprets the Daily local backup job in the time zone of the DataFabric Manager server, therefore, the backup starts at 1:00 p.m. Monday, Lagos time (8:00 p.m. Hong Kong time).
- Protection Manager interprets the Daily remote backup job in the time zone of the DataFabric Manager server, therefore, the remote backup starts at 4:00 p.m. Monday, Lagos time (11:00 p.m. Hong Kong time). Protection Manager starts the backup, replicating primary data in Nigeria to backup destination storage in Los Angeles.
- Protection Manager interprets the Weekly mirror copy job in the time zone of the DataFabric Manager server, therefore, remote mirroring starts at 2:30 a.m. Monday, Los Angeles time (6:30 p.m. Hong Kong time). Protection Manager mirrors the data, replicating the backed-up data on the secondary storage in the U.S. to tertiary storage in Lima.

The location and time zone of the tertiary destination storage does not impact the schedule.





## Types of schedules

---

You can configure reusable protection schedules (that specify times to carry out data backup and mirror operations) and throttle schedules (that specify periods of unlimited, limited, or zero network bandwidth availability for those operations).

Protection and throttle schedules are assigned to protection policies to determine when the backup or mirror operations that are specified in the policies are carried out.



# Summary of schedule features

---

The licensed protection application provides the following protection and throttle schedule features:

<b>Hourly, Daily, Weekly, and Monthly backup or mirror operations</b>	For complex scheduling and retention purposes, you can schedule Hourly, Daily, Weekly, and Monthly classes of backup or mirror operations (also called events).
---	---

**Note:** Despite their labels, Hourly, Daily, Weekly, and Monthly backup or mirror operations do not necessarily take place once an hour, once a day, once a week, or once a month.

Hourly events can also be scheduled at intervals that are greater or less than an hour.

Daily events can be scheduled multiple times a day.

Weekly events can be scheduled multiple times a week.

Monthly events can be scheduled multiple times a month.

<b>Daily, Weekly, or Monthly protection schedules</b>	You configure Daily, Weekly, or Monthly protection schedules to contain your backup or mirror operations.
	<ul style="list-style-type: none"> <li>• Daily protection schedules specify all backup or mirror operations to take place in a day. They can include both Hourly and Daily operations.</li> <li>• Weekly protection schedules specify your Weekly operations and also incorporate the Hourly and Daily operations in one or more existing Daily protection schedules.</li> <li>• Monthly protection schedules can specify your Monthly operations and also incorporate the Weekly, Daily, and Hourly operations in any existing Weekly or Daily schedule.</li> </ul>

<b>Hourly, Daily, Weekly, or Monthly backup copy retention</b>	Your Hourly, Daily, Weekly, or Monthly backup operations produce Hourly, Daily, Weekly, or Monthly classes of backup copies. For retention purposes, you can assign different retention times to each of these classes of backup copies when you configure the protection policy. For example, you can choose to retain your Hourly backup copies just a short duration of 24 hours, and retain your Daily backup copies for a longer 7 day duration.
--	---

<b>Bandwidth throttle periods</b>	You can specify periods of unlimited, limited, or no network bandwidth availability to carry out remote backup or mirror operations.
-----------------------------------	--

<b>Reusability</b>	You can reuse protection and throttle schedules. When you configure protection policies, you can apply the same schedule to multiple primary data nodes, backup connections, or mirror connections in multiple policies.
--------------------	--



# Configuration sequence for schedules, policies, and datasets

---

If you are using the licensed protection application to customize your data protection, you must configure the schedule, policy, and dataset components in a specific order because some components are put together using other components.

Configure the schedule, policy, and dataset components in the following order to configure your data protection.

## 1. Daily Schedule

The configuration specifies hourly and daily backup or mirror times for a 24-hour period.

Configuration prerequisites: None.

Postconfiguration assignments: Protection policies, or weekly schedules, or monthly schedules.

## 2. Weekly Schedule (optional)

The configuration specifies hourly, daily, and weekly backup or mirror times for Sunday through Saturday.

Configuration prerequisites: Optional daily schedule. In some instances, you might want to create weekly schedules for the specific purpose of scheduling weekly backup or mirror operations. In such cases, daily schedules are not prerequisites.

Postconfiguration assignments: Protection policies, or Monthly schedules.

## 3. Monthly Schedule (optional)

The configuration specifies hourly, daily, weekly, and monthly backup and mirror times for a month.

Configuration prerequisites: Optional daily or weekly schedule. In some instances, you might want to create monthly schedules for the specific purpose of scheduling monthly backup or mirror operations. In such cases, daily or weekly schedules are not prerequisites.

Postconfiguration assignments: Protection policies.

## 4. Throttle Schedule (optional)

The configuration specifies periods of unlimited, limited, or no network bandwidth availability for backup or mirror operations.

Configuration prerequisites: None.

Postconfiguration assignments: Protection policies.

## 5. Protection Policy

The configuration specifies type of protection, backup retention durations, backup scripts, protection topology, daily, weekly, or monthly backup and mirror schedules, and throttle schedules.

Configuration prerequisites: Daily, weekly schedules, or monthly schedules, and throttle schedules (if bandwidth throttle times are required). Though protection policies do not require protection schedules assigned to them, the usual practice is to assign protection schedules to specify times for backup and mirror operations.

Postconfiguration assignments: Datasets.

**6. Resource Pool (optional)**

The configuration specifies data storage elements.

Configuration prerequisites: None.

Postconfiguration assignments: Datasets.

**7. Dataset**

The configuration specifies protection policy, dataset members, primary data node, backup node, or mirror node sites.

Configuration prerequisites: Protection policies and resource pools. (If you want to assign a resource pool to a dataset, you must have that resource pool configured before you configure the dataset. )

Postconfiguration assignments: None.

# Planning schedules for protection policy nodes and connections

---

You can assign schedules to the primary data node, backup connection, or mirror connection of a protection policy. The licensed protection application uses the assigned schedules to carry out the configured data protection operations (local backup, remote backup, or mirror) appropriate to that node or connection.

## Next topics

[\*Planning a schedule for the primary data node\*](#) on page 293

[\*Planning a schedule for a backup connection\*](#) on page 294

[\*Planning a schedule for a mirror connection\*](#) on page 294

## Related concepts

[\*Effect of time zones on schedules\*](#) on page 1049

## Planning a schedule for the primary data node

On the primary data node, protection schedules specify the times to perform local backups.

Typically, schedules assigned to the primary data node specify times for Hourly local backups at regular intervals. These backups are good for quick restoration of recent data that might have been deleted or corrupted by accident. Consider the following questions.

**Note:** Primary data nodes containing Open Systems SnapVault directories do not support local backup.

- How frequently do I need to execute a local backup?

The less you can afford to lose recent data due to accidental deletion or data corruption, the more frequently you need to execute local backup.

- How long do I need to retain a local backup?

Typically Hourly local backups are retained for at least a 24-hour period, at least until a Daily remote backup to secondary storage is executed.

- Do I need to retain some local backups longer than others?

If you do, then you need to plan on scheduling both Hourly and Daily classes of backups.

- Do I want to vary my local backup schedule on weekends?

If you do, then you want to apply at least a weekly schedule that includes a daily schedule of frequent backups on weekdays and a daily schedule of infrequent backups on weekends.

## Planning a schedule for a backup connection

For backup connections, schedules specify the times to perform remote backups from a source to the secondary or tertiary backup storage.

Typically, schedules assigned to a backup connection specify times for one or two daily remote backups after working hours or during periods of low data input activity. Daily remote data backup ensures that data loss due to storage system damage at the backup source can be restored from secondary or tertiary storage with only a day or less of data loss. Consider the following questions.

- How frequently do I need to execute a remote backup?  
The less you can afford to lose recent data due to damage of the primary data node, the more frequently you need to backup.
- How long do I need to retain a backup on the backup node?  
Typically daily remote backups are retained for at least a seven-day period, at least until a Weekly remote backup to secondary or tertiary storage is executed.
- Do I need to retain some backups longer than others?  
If you do, then you need to plan on scheduling both Daily and Weekly classes of backups.
- Do I want to vary my remote backup schedule on weekends?  
If you do, then you want to apply at least a weekly schedule that includes a daily schedule of frequent backups on weekdays and a daily schedule of infrequent backups on weekends.

## Planning a schedule for a mirror connection

For mirror connections, schedules specify the times to perform mirror operations from a source to the destination storage.

Typically, schedules assigned to a mirror connection specify times for one or two daily mirror operations after working hours or during periods of low data input activity. Daily mirror backup ensures that data loss due to storage system damage at the source site can be quickly be restored or at least made available from the mirror target site. Consider the following questions.

- How frequently do I need to execute a mirror operation?  
The less you can afford to lose recent data or have it unavailable, the more frequently you need to execute mirror operations.
- Do I want to vary my mirror schedule on weekends?  
If you do, then you want to apply at least a weekly schedule that includes a daily schedule of frequent mirror operations on weekdays and a daily schedule of infrequent mirror operations on weekends.

# Description of daily, weekly, and monthly protection schedules

---

You can configure daily, weekly, and monthly protection schedules to specify times for your backup or mirror operations over a day-long, week-long, or month-long period.

## Daily protection schedules

Daily protection schedules specify times for hourly backup and mirror operations and times for daily backup and mirror operations over a 24-hour period.

### Hourly backup and mirror operations

Hourly backup and mirror operations are the backups that you schedule by time period and frequency. They are executed at regular intervals (hourly or subhourly, usually during work hours) on a daily basis when you set up a daily schedule.

A common practice is to apply a schedule of frequent hourly local backup and remote backup operations on the primary node and on the backup connection between the primary node and secondary backup node.

### Daily backup and mirror operations

Daily backup and mirror operations are executed on a daily basis (usually during nonwork hours) at specific times that you specify when you set up a daily schedule.

A common practice is to apply a schedule of one or two daily local backup and remote backup operations per day on the primary node and on the backup connection between the primary node and secondary backup node.

## Weekly protection schedules

A weekly protection schedule usually consists of one or more daily schedules that apply to specific days over the seven-day week. For example, you might include a daily schedule of frequent backups to run from Monday through Friday and a different daily schedule of infrequent backups to run on Saturdays and Sundays.

When you set up a weekly schedule, you can schedule the hourly and daily backup and mirror operations that are specified in the assigned daily schedules. You can also schedule weekly backup and mirror operations. Weekly backup and mirror operations are specified by a specific day and time.

A common practice is to apply a schedule of one or two weekly local backup and remote backup operations on the primary node and on the backup connection between the primary node and secondary backup node or secondary and tertiary backup node.

## Monthly protection schedules

A monthly protection schedule is executed on a monthly basis at specific times that you specify when you set up a monthly schedule. You can schedule backup and mirror

operations over a month-long period by specifying either an existing daily schedule or an existing weekly schedule to be repeated over this period.

When you set up a monthly schedule, you can include the hourly, daily, or weekly backup or mirror operations that are specified in the applied daily or weekly schedule. You can also schedule monthly backup or mirror operations by specifying a day and time usually, once or twice a month.

A common practice is to apply a schedule of one or two monthly remote backup operations between secondary storage and tertiary storage.

## Throttle schedules and network bandwidth

---

A throttle schedule enables you to configure periods of unlimited, limited, or zero network bandwidth availability for your data backup or mirror operations.

During times of heavy general network usage, you might want to limit the network bandwidth used by your backup or mirror operations. Conversely, during times of light network usage, you might want to leave unlimited bandwidth available for your protection operations.

If you want to stop all backup or mirror activity over a connection during a time period, use the throttle schedule to assign zero availability to a backup or mirror connection during that period. During a period of zero availability no backup or mirror operations can start and all backup or mirror operations in progress when that period began are aborted and restarted at the end of the period of zero availability.

**Note:** Backup or mirror operations that are in progress when a new period of limited bandwidth begins continue to completion using their original bandwidth allotment. Backup or mirror operations that start during a period of limited bandwidth allotment execute using that bandwidth limit.

**Note:** When the licensed protection application executes a mirror operation that consists of multiple simultaneous data transfers, the application divides the total bandwidth allotted to this operation and distributes it equally to each transfer.



# Throttle schedule properties

---

You can use the following definitions when you configure or edit a throttle schedule.

<b>Name</b>	The name of the throttle schedule.
<b>Start Time</b>	The hour and minute that a bandwidth allotment period begins when this schedule is applied. Click the up or down arrow to modify the start time. As you change the start time, the throttle period displayed on the graphed schedule changes accordingly.
<b>End Time</b>	The hour and minute that a bandwidth allotment period ends when this schedule is applied. Click the up or down arrow to modify the end time. As you change the end time, the throttle period displayed on the graphed schedule changes accordingly.
<b>Throughput</b>	<p>The network bandwidth, in kilobytes per second, that are allotted to an assigned backup operation during this throttle period. For graphing purposes, bandwidth availability is rounded up to the nearest kilobyte per second. When the licensed protection application executes a mirror operation that consists of multiple simultaneous data transfers, the application divides the total bandwidth allotted to this operation and distributes it equally to each transfer.</p> <ul style="list-style-type: none"><li>• The default setting is no limit on the bandwidth allotted the backup or mirror operation.</li><li>• Allotting zero megabytes per second to a throttle period stops any remote backup or mirror operation in progress or scheduled to start during that throttle period.</li><li>• Allotting limited bandwidth to a throttle period causes any backup or mirror operations that start within the period to execute using the allotted bandwidth. Backup or mirror operations that are in progress when a new period of limited bandwidth begins, continue to completion using their original bandwidth allotment.</li></ul>
<b>Delete</b>	Deletes a throttle period from the schedule.
<b>Add</b>	Adds a row of Start Time, End Time, and Throughput fields to specify an additional throttle period for this schedule.



# Protection schedules and time zones

---

If the DataFabric Manager server that hosts the licensed protection application is located in a time zone different from the primary data node, backup node, or mirror node, the difference in time zone settings for the dataset or physical resource pool elements of those nodes might affect the execution of the protection or throttle schedules that you assign in your protection policy.

If a policy node's dataset or physical resource pool elements are not assigned a time zone setting, then by default the licensed protection application executes the protection schedule for that node or its backup or mirror connection in accordance with the clock and time zone setting on the DataFabric Manager server.

For example, without time zone settings on the primary data node datasets, a daily backup scheduled for 9 p.m. (Eastern Standard Time) from a protection application console and a DataFabric Manager server in New York will, by default, execute at 6 p.m. (Pacific Standard Time) on a primary data node in Los Angeles, or at 2 a.m. (GMT) at a primary data node in London.

However, if those Los Angeles and London datasets are assigned Pacific Standard Time and GMT time zone settings respectively, then the protection application adjusts the schedule to execute daily backups at 9 p.m. (Pacific Standard Time) in Los Angeles and at 9 p.m. (GMT) in London.

## Related concepts

[What a protection policy is](#) on page 847

[Effect of time zones on schedules](#) on page 1049



# Decisions to make before adding a schedule

---

Before you use the **Add Schedule** wizard to add a new protection or throttle schedule to your list of existing schedules, you must make some decisions about the need for and the type of schedule that you want to create.

## Preliminary schedule decisions

- Can the protection policies that you want to apply use their currently assigned schedules? If not, do you want to apply different daily, weekly, monthly, or throttle schedules to the primary node, backup connection, or mirror connection components of those protection policies?
- If a policy requires a different daily, weekly, monthly, or throttle schedule, can you assign an existing schedule of that type, or do you need to create a new schedule?
- If you need to create a new schedule, what is its name and description?

## Daily schedule creation decisions

If you need to add a daily schedule, make the following decisions before starting the **Add Schedule** wizard:

- Do you want to use this daily schedule for specifying hourly backup and mirror operations and, if so, over what hours and at what time intervals?  
A common practice is to schedule frequent hourly backup and mirror operations at the Primary Data node during working hours or periods of heavy data input.
- Do you want to schedule hourly backup operations at intervals shorter than an hour?  
Protection configurations on which you plan to schedule backup operations at intervals of less than an hour require that both the source and destination nodes are preconfigured with the SnapMirror license.
- Do you want daily backups for retention purposes, and if so, at what times in the day?  
When you apply this schedule to a protection policy node, you can assign different retention durations to your hourly and daily backups. A common practice is to schedule one or two daily backup operations per day, at least one of which is during nonworking hours.
- Do you want to schedule daily mirror operations at odd times in addition to the regular hourly mirror operations that you will set up in this schedule?

## Weekly schedule creation decisions

If you need to add a weekly schedule, make the following decisions before starting the **Add Schedule** wizard:

- Do you want to apply existing daily schedules to this weekly schedule? If so, for which days of the week (for example, Daily schedule A: Saturday through Sunday, Daily schedule B: Monday through Friday)?  
The hourly and daily backups in the applied daily schedules are automatically included in the new weekly schedule.
- Do you want weekly backups for retention purposes?  
When you apply this schedule to a protection policy node, you can assign different retention durations to your hourly, daily, and weekly backups.
- Do you want to schedule weekly mirror operations at odd times in addition to the times already specified for the hourly or daily mirror operations of the applied daily schedules?
- Which days and times during the week do you want to schedule weekly backup or mirror operations?  
A common practice is to schedule one or two weekly backups per week.

### Monthly schedule creation decisions

If you need to add a monthly schedule, make the following decisions before starting the **Add Schedule** wizard:

- Do you want to apply an existing daily or weekly schedule to this monthly schedule?  
The hourly, daily, and weekly backup and mirror operations in the applied daily or weekly schedule are automatically included in the new monthly schedule.  
If you specify a daily schedule, that schedule applies to every day of the month; if you specify a weekly schedule, that schedule applies to every week of the month.
- Do you want monthly backups for retention purposes?  
When you apply this schedule to a protection policy node, you can assign different retention durations to your hourly, daily, weekly, and monthly backups.
- Do you want to schedule monthly mirror operations at odd times outside the times already specified for the hourly, daily, or weekly mirror operations of the applied daily or weekly schedules?
- Which days and times during the month do you want to schedule monthly backup or mirror operations?  
A common practice is to schedule one or two monthly backups per month.

### Throttle schedule creation decisions

Data protection operations can consume large amounts of network bandwidth. If you need to create a schedule to throttle the bandwidth availability used by these operations, make the following decisions before starting the **Add Schedule** wizard:

- Do you want to restrict the network bandwidth available for backup or mirror operations at certain times of the day?
- Do you want to prevent new backup or mirror operations completely, at certain times of the day?  
Zero network bandwidth allotment prevents all new backup or mirror operations during the period and on the connection in which it is in effect.

**Note:** When the licensed protection application executes a mirror operation that consists of multiple simultaneous data transfers, the application divides the total bandwidth allotted to this operation and distributes it equally to each transfer.



# Adding a daily protection schedule

---

You can use the **Add Schedule** wizard to create new daily protection schedules. After you create a daily schedule, you can apply it to protection policies to determine when hourly and daily backup or mirror operations are executed.

## Before you begin

Have the information available that you need to complete this task:

- Time to perform the mirror or backup operation and how often (required)
- Retention time of mirror or backup copies (optional)
- Throttle schedule (optional)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Click **Add** to start the **Add Schedule** wizard.
3. In the wizard, select the **Daily** schedule option and complete the wizard to create the new Daily schedule.

If you do not want to include hourly backup or mirror operations in this schedule, continue past the Hourly Events property sheet without specifying a time.

Your new schedule is listed on the Schedules tab.

## Related concepts

*Decisions to make before adding a protection policy* on page 251

## Related references

*Administrator roles and capabilities* on page 1055



# Adding a weekly protection schedule

---

You can use the **Add Schedule** wizard to create new weekly protection schedules. After you create a weekly schedule, you can apply it to protection policies to determine when hourly, daily, and weekly backup or mirror operations are executed.

## Before you begin

Have the information available that you need to complete this task:

- Days and time to perform the mirror or backup operation and how often (required)
- Retention time of mirror or backup copies (optional)
- Throttle schedule (optional)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Click **Add** to start the **Add Schedule** wizard.
3. In the wizard, select the **Weekly** schedule option and complete the wizard to create the new Weekly schedule.

If you do not want to schedule weekly backups, continue past the Weekly Events property sheet without specifying a day or time.

Your new schedule is listed on the Schedules tab.

## Related concepts

*Decisions to make before adding a protection policy* on page 251

## Related references

*Administrator roles and capabilities* on page 1055



# Adding a monthly protection schedule

---

You can use the **Add Schedule** wizard to create new monthly protection schedules. After you create a monthly schedule, you can apply it to protection policies to determine when hourly, daily, weekly, and monthly backup or mirror operations are executed.

## Before you begin

Have the information available that you need to complete this task:

- Days and time to perform the mirror or backup operation and how often (required)
- Retention time of mirror or backup copies (optional)
- Throttle schedule (optional)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Click **Add** to start the **Add Schedule** wizard.
3. In the wizard, select the **Monthly** schedule option and complete the wizard to create the new monthly schedule.

Your new schedule is listed on the Schedules tab.

## Related concepts

*[Decisions to make before adding a protection policy](#)* on page 251

## Related references

*[Administrator roles and capabilities](#)* on page 1055



# Adding a throttle schedule

---

You can use the **Add Schedule** wizard to create new throttle schedules. After you create a throttle schedule, you can apply it to protection policies to schedule periods of unlimited, limited, or no network bandwidth availability for remote backup or mirror operations.

## Before you begin

Have the information available that you need to complete this task:

- Days and time to restrict the network bandwidth for backup or mirror operations.
- Days and times to prevent backup or mirror operations.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Click **Add** to start the **Add Schedule** wizard.
3. In the wizard, select the **Throttle** schedule option and complete the wizard to create the new throttle schedule.

Your new schedule is listed on the Schedules tab.

## Related concepts

*[Decisions to make before adding a protection policy](#)* on page 251

## Related references

*[Administrator roles and capabilities](#)* on page 1055



# Editing a daily schedule

---

You can edit a daily protection schedule to modify the hourly backup and mirror times and the daily backup or mirror times.

## Before you begin

Have the information available that you need to complete this task:

- Times for hourly backup or mirror operations.
- Times for daily backup or mirror operations.

If you plan to schedule backup operations at intervals of less than one hour, confirm that both the source and destination nodes are configured with a SnapMirror rather than a SnapVault license.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

Be aware that when you apply this schedule to a node or connection in a policy, the actual times of your scheduled backup or mirror operations are affected by the time zone location of the source node in relation to the time zone location of the DataFabric Manager server and the time zone setting of the dataset or physical resource assigned to the source node.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Select the daily schedule that you want to edit and look at the Dependencies list to view all the weekly schedules, monthly schedules, or protection policies that use this schedule.

Make sure that the edits that you plan to make to the schedule are appropriate for all the dependencies in the list.

3. With the daily schedule that you want to edit still selected, click **Edit**.

The General tab on the **Properties** sheet displays a graph of the scheduled events. Depending upon the protection policy and the policy node or connection to which you apply this schedule, the times shown on the graph schedule either local backups (on the primary data node) or backup or mirror copies (for backup connections or mirror connections).

4. To change the name or description of the schedule, edit the Name or Description parameters and click **Apply**.
5. To configure hourly backup or mirror times, click **Hourly Events**, then click **Add**.
  - a. Double-click the **Start Time** and **End Time** columns, then use the up and down arrows in the newly added time entry to specify a time period for hourly backup or mirror operations.

The period timeline in the graph adjusts to display more or fewer hours according to the changes you make.

- b. Double-click **Frequency** and enter the frequency, in minutes, that an hourly backup will take place within this time period.
  - c. Click **Apply** to confirm the changes to the schedule.
6. To configure daily backup or mirror times, click **Daily Events**, then click **Add**.
- a. Use the up and down arrows in the newly added time entry to specify a time period for daily backup or mirror operations.
- The period timeline in the graph adjusts to display more or fewer hours according to the changes you make.
- b. Click **Apply** to confirm the changes to the schedule.
7. To delete an existing time period from this schedule, click **Hourly Events** or **Daily Events**, then select the schedule and click **Delete**.
8. Click **OK** to finalize your changes to this daily schedule.

You can include this daily protection schedule in a weekly or monthly protection schedule or you can assign it directly to a protection policy's primary data node, backup connection, or mirror connection elements. When you assign this schedule to a policy, you can assign different retention durations for the hourly and daily backup copies produced by this schedule.

#### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Editing a weekly schedule

---

You can edit a weekly protection schedule to modify the daily and weekly backup and mirror operations.

## Before you begin

Have the information available that you need to complete this task:

- Times for weekly backup or mirror operations.
- Changes to a daily schedule used by this weekly schedule.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

Be aware that when you apply this schedule to a node or connection in a policy, the actual times of your scheduled backup or mirror operations are affected by the time zone location of the source node in relation to the time zone location of the DataFabric Manager server and the time zone setting of the dataset or physical resource assigned to the source node.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Select the weekly schedule that you want to edit and look at the Dependencies list to view all the monthly schedules or protection policies that use this schedule.

Make sure that the edits that you plan to make to the schedule are appropriate for all the dependencies in the list.

3. With the weekly schedule that you want to edit still selected, click **Edit**.

The General tab on the **Properties** sheet displays a graph of the scheduled events.

4. To change the name or description of the schedule, edit the Name or Description parameters and click **Apply**.
5. To configure or modify daily backup or mirror times, click **Daily Events**. To configure a new daily backup or mirror schedule, click **Add**.
  - a. Double-click the **Start Day** and **End Day** columns and use the up or down arrows to specify the first and last day of the week on which to apply an existing daily schedule (for example, Monday and Friday).
  - b. Double-click **Daily Schedule** and select the daily schedule that you want to apply within these weekly start and end days.

Your weekly schedule automatically schedules the hourly and daily backup or mirror operations that are specified in the assigned daily schedule.

- c. Click **Apply** to confirm the changes to the schedule.
6. To configure or modify weekly backup or mirror times, click **Weekly Events**. To configure a new weekly backup or mirror schedule, click **Add**.
  - a. Double-click the **Event Day** and **Event Time** columns and use the up or down arrows to specify a day and a time.
  - b. Click **Apply** to confirm the changes to the schedule.
7. To delete an existing time period from this schedule, click **Daily Events** or **Weekly Events**, then select the schedule and click **Delete**.
8. Click **OK** to finalize your changes to this weekly schedule.

You can include this weekly protection schedule in a monthly protection schedule or you can assign it directly to a protection policy's primary data node, backup connection, or mirror connection elements. When you assign this schedule to a policy, you can assign different retention durations for the hourly, daily, and weekly backup copies produced by this schedule.

#### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Editing a monthly schedule

---

You can edit a monthly protection schedule to modify the daily, weekly, and monthly backup and mirror operations.

## Before you begin

Have the information available that you need to complete this task:

- Times for monthly backup or mirror operations.
- Changes to a daily or weekly schedule used by this monthly schedule.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

Be aware that when you apply this schedule to a node or connection in a policy, the actual times of your scheduled backup or mirror operations are affected by the time zone location of the source node in relation to the time zone location of the DataFabric Manager server and the time zone setting of the dataset or physical resource assigned to the source node.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Select the monthly schedule that you want to edit and look at the Dependencies list to view all the protection policies that use this schedule.

Make sure that the edits that you plan to make to the schedule are appropriate for all the dependencies in the list.

3. With the monthly schedule that you want to edit still selected, click **Edit**.

The General tab on the **Properties** sheet displays a graph of the scheduled events.

4. To change the name or description of the schedule, edit the Name or Description parameters and click **Apply**.
5. To edit the daily or weekly schedule assignments for this monthly schedule, click **General**, make the changes, then click **Apply**.
6. To configure or modify daily or weekly schedule assignments, click **Monthly Events**. To configure a new monthly backup or mirror schedule, click **Add**.
  - a. Double-click the entries you want to edit and use the up or down arrows to select new values.
  - b. Click **Apply** to confirm the changes to the schedule.
7. To delete an existing entry from this schedule, click **Monthly Events**, then select the schedule and click **Delete**.

- 8.** Click **OK** to finalize your changes to this monthly schedule.

You can assign this monthly protection schedule directly to a protection policy's primary data node, backup connection, or mirror connection elements. When you assign this schedule to a policy, you can assign different retention durations for the hourly, daily, and weekly, and monthly backup copies produced by this schedule. You can assign this Monthly protection schedule directly to a protection policy's primary node, backup connection, or mirror connection elements.

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Editing a throttle schedule

---

You can edit an existing throttle schedule to increase or limit the connection bandwidth allotted to remote backup or mirror operations.

## Before you begin

Have the information available that you need to complete this task:

- Days and time to restrict the network bandwidth for backup or mirror operations.
- Days and times to prevent backup or mirror operations.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

Be aware that when you apply this throttle schedule to a backup connection or mirror connection in a policy, the actual start and end times of your throttle periods are affected by the time zone location of the backup or mirror source nodes in relation to the time zone location of the DataFabric Manager server and the time zone setting of the datasets or physical resources assigned to the source nodes.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.

2. Select a throttle schedule and click **Edit**.

The throttle schedule **Properties** sheet displays a graph of the schedule that shows the periods of limited or no network bandwidth availability. For graphing purposes, bandwidth availability is rounded up to the nearest kilobyte per second.

3. To add a throttle time, click **Add**.
4. To edit a new or existing throttle time, select the entry, then double click the entry in each column and select or enter a new setting
5. Click **OK** to finalize your changes to this throttle schedule.

You can assign this throttle schedule to a protection policy's backup connection or mirror connection components.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a protection or throttle schedule

---

You can delete daily, weekly, monthly or throttle schedules.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Select the schedule that you want to delete and look at the Dependencies list to view any protection policies or other schedules to which this schedule is assigned.

**Note:** You cannot delete a schedule if it is used by protection policies or other schedules. If any are listed in the Dependencies list, you must first stop this procedure and edit the listed policies and schedules so that they no longer use this schedule.
3. If no dependencies are listed, click **Delete**, then click **Yes**.

The selected schedule is deleted.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Assigning or changing schedules in a protection policy

---

You can assign or change protection and throttle schedules for the primary node, backup connection, or mirror connection of a protection policy.

## Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Confirm that time zone differences and settings on the DataFabric Manager server, and the dataset or physical resource pool elements of the policy nodes support the new schedule assignment.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Select the protection policy that has the local backup, remote backup, or mirror schedule assignment you want to modify and click **Edit > Nodes and Connections**.
3. Select the primary node, backup connection, or mirror connection that you want to modify.
4. Locate the appropriate schedule in the Properties area (Local Backup Schedule, Backup Schedule Name, Mirror Schedule Name, or Throttle Schedule Name) and select a new schedule from the schedule drop-down list.
5. After you complete your modifications, click **Preview**.
6. Review the effects of your changes and do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the **Properties** sheet.

The modifications take effect immediately.

## Related tasks

[How do I back up data?](#) on page 589

## Related references

[Administrator roles and capabilities](#) on page 1055



# Copying a protection or throttle schedule

---

You can quickly create copies of your a daily, weekly, monthly or throttle schedule. After copying a schedule, you can customize it to your particular needs.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Protection > Schedules**.
2. Select the schedule that you want to copy and click **Copy**.

A copy of the selected schedule appears with "Copy of .." appended to the original schedule name. The licensed protection application selects and highlights the new "Copy of.." schedule for editing.

Click **Edit** to rename and customize the new schedule copy as needed.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Dataset concepts

---

You can use datasets to group data and use resource pools to group storage to simplify the monitoring, provisioning, reporting, and access control of your SnapVault and SnapMirror relationships, which enables flexible and efficient use of storage.

Associating a data protection, disaster recovery, or provisioning policy with a dataset lets storage administrators automate tasks, such as assigning consistent policies to primary data, propagating policy changes, and provisioning new volumes, qtrees, or LUNS on primary and secondary dataset nodes. The licenses that you have installed determine which policies are available.

Configuring a dataset combines the following objects:

<b>Dataset</b>	For protection purposes, a dataset is a collection of physical resources on a primary node, such as volumes, flexible volumes, and qtrees, and copies of backed-up data.  <b>Note:</b> It is a good practice to group primary data that have identical data protection requirements.
	For provisioning purposes, a dataset is a collection of physical resources, such as volumes, flexible volumes, qtrees, and LUNs, that are assigned to a dataset node. If the protection license is installed and the protection policy establishes a primary and one or more nonprimary nodes, each node of the dataset is a collection of physical resources that might or might not be provisioned from the same resource pool.
	A dataset cannot contain a storage system that is also in a resource pool assigned to a dataset node. This constraint prevents a loop that attempts to provision an infinite number of volumes.
<b>Application dataset</b>	A dataset managed by an application that is external to the licensed protection and provisioning applications, such as a dataset managed by SnapManager for Oracle.
<b>Resource pool</b>	A collection of physical resources from which secondary storage is provisioned. Resource pools can be used to group storage systems and aggregates by attributes, such as performance, cost, physical location, or availability.
<b>Data protection policy</b>	A data protection policy defines how to protect the primary, secondary, and tertiary storage, as well as when to create copies of data and how many copies to keep.
<b>Provisioning policy</b>	A provisioning policy defines how to provision primary or secondary dataset nodes, and provides rules for monitoring and managing storage space and for allocating storage space from available resource pools.

## Related concepts

[Overview of resource pools](#) on page 819

*What a policy is* on page 847

*What groups are* on page 1047

## How the protection application uses datasets

---

The licensed protection application uses the information in a dataset to create Snapshot copies used for backups and mirror copies, to provision storage as needed for the copies, and to transfer the copies to backup or mirror nodes.

After you set up a dataset for protection, the licensed protection application performs the following operations:

1. The application provisions volumes and qtrees on the destination node in several ways. For storage systems that run Data ONTAP 7.0 or later, the application automatically provisions flexible volumes and qtrees when the resource pool contains an aggregate. For storage systems that run Data ONTAP 6.5 or earlier, you manually add secondary storage to the destination node. If you manually select storage without using resource pools for a SnapMirror destination node, the application provisions traditional volumes assigned to that destination node.
2. The application creates backup relationships (either SnapVault or SnapMirror) between volumes and qtrees in the dataset with the newly provisioned secondary storage.
3. The application runs the data protection schedules, making Snapshot copies of the primary data and initiating SnapVault and SnapMirror baseline transfers at the scheduled times.
4. The application periodically checks that the dataset conforms to its data protection policy. If either the dataset membership or the policy changes, the application tries to bring the dataset back into conformance, or it notifies you that the conformance status changed to nonconformant.



# How the provisioning application works with datasets

---

The licensed provisioning application simplifies and automates the tasks of provisioning and managing storage for the data in datasets.

After you add a dataset for provisioning, the licensed provisioning application performs the following operations:

- Provisions the dataset

The application provisions volumes and qtrees (in NAS environments) or volumes and LUNs (in SAN environments) for a dataset using the resource pool assigned to the dataset. In SAN environments, a provisioned volume can be delegated to SDx applications and used to create qtrees or LUNs.

If you have the provisioning license only, the primary dataset node is provisioned.

If you also have the protection license, the licensed provisioning application can provision volumes, qtrees, or LUNs on the backup and mirror dataset nodes.

**Note:** You are advised NOT to use SnapDrive for Windows versions lower than 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error requiring the LUNs to be manually unmapped.

- Configures automatic storage using policies and templates

When you create a dataset for provisioning, you can assign a provisioning policy that provides settings for automatically configuring storage for the dataset.

- Allows manual addition of storage space

You can manually add additional volumes, qtrees, or LUNs, at any time, to a dataset that has a provisioning policy assigned.

- Handles dataset-managed protocols for exporting data

Protocols for exporting data are automatically handled by the dataset.

You can also assign a vFiler template to a vFiler host. When a vFiler host is created, the vFiler template provides default settings for automatically configuring the vFiler host.

- Checks for conformance

The application periodically checks that the dataset conforms to its provisioning policy. For example, if the data in a dataset reaches a specified threshold level, the application tries to create additional space according to the provisioning policy, either by increasing the storage container size or deleting old Snapshot copies, or both. If it cannot bring the dataset back into conformance, it notifies you that the conformance status changed to nonconformant.

- Allows manual management of storage space

The application provides manual controls for viewing and resizing individual volumes or qtrees and modifying volume data and Snapshot copy space allocations.



# About NFS, CIFS, iSCSI, or FC protocol access

---

You can configure NFS, CIFS, iSCSI, or Fibre Channel (FC) export protocols for client access to a dataset.

You can specify support for export protocol access when you create a dataset, when you reconfigure the primary, backup, or mirror nodes in your dataset, or when you provision a new volume, LUN, or qtree into the dataset.

There are two ways that you can export storage in a dataset.

You can enable one export protocol for an entire primary, backup, or mirror node of a dataset. Clients can access all of the storage, that is all volumes, qtrees, and LUNs, in a particular dataset node by using the specified protocol.

To achieve this configuration, specify export settings for the primary node when completing the **Add Dataset** wizard and for the backup and mirror nodes by using the **Dataset Policy Change** wizard.

You can assign different export protocols to each new volume, LUN, or qtree member when you provision the member into a dataset, rather than specifying an export protocol for the entire dataset node. Clients can selectively access dataset members, based on the protocols enabled for each client and each dataset member.

To achieve this configuration, do not specify an export protocol when creating a dataset. Instead, use the **Provisioning** wizard to provision a new member into a dataset and select the option to export the new member.

**Note:** The export settings presented in the **Provisioning** wizard are determined by the provisioning policy type assigned to the dataset.

## Related concepts

[Overview of export protocol properties](#) on page 743

## Related tasks

[Configuring dataset nodes for NFS protocol access](#) on page 747

[Configuring dataset nodes for CIFS protocol access](#) on page 745

[Configuring dataset nodes for FC protocol access](#) on page 749

[Configuring dataset nodes for iSCSI protocol access](#) on page 751



# When to configure datasets

---

You should configure datasets when you have identified which data to group for protection or provisioning.

You can also configure datasets in the following situations:

## Protection

- You installed the protection license and are setting up data protection for the first time.
- You previously used Backup Manager or Disaster Recovery Manager and are upgrading to the licensed protection application, and you want to import existing relationships that the licensed application discovered.
- You never used Operations Manager to monitor or manage your SnapVault or SnapMirror relationships and want to import existing relationships that the licensed protection application discovered.
- A condition changed that affects the status of the dataset, and you want to change the protection policy.
- You are monitoring your storage resources by viewing the dashboard, which displays resources as well as which resources are unprotected.
- You added a storage system, or DataFabric Manager discovered it, and you want to protect the data on that storage system.

## Provisioning

- You installed the provisioning license and are setting up provisioning for the first time.
- You want to provision an existing dataset that has not yet been provisioned.
- You need to add another volume or LUN to an existing dataset.
- A condition changed that affects the status of the dataset, and you want to change the provisioning policy.
- You are monitoring your storage space usage by viewing the dashboard and it displays a warning for a dataset member that is running out of space.



## How to enable backup of multiple primary volumes to a single secondary volume

---

You can configure your protection application to support SnapVault-based or Qtree SnapMirror-based backup of multiple volumes in primary storage to a single volume in secondary storage.

By default, the protection application automatically sets up one-to-one backup relationships between primary and secondary volumes when provisioning secondary nodes in datasets. But in circumstances in which the 500-volume limit for storage systems might not allow a one-to-one ratio of primary volumes to secondary volumes, you can configure the protection application through the Operations Manager global option `dpMaxFanInRatio` (to support backup relationships between multiple volumes in primary storage and a single volume in secondary storage).

**Note:** The following limitations apply to protection application support for automatically configuring backup relationships of multiple primary volumes to a single secondary volume when provisioning secondary storage:

- The protection application does not support volume SnapMirror-based mirroring from multiple primary volumes to a single secondary volume.
- All the primary volumes and the secondary volume must be members of the same dataset.
- The protection application implementation of Open Systems SnapVault backup is not affected by the `dpMaxFanInRatio` option.

For more information on the `dpMaxFanInRatio` global option, see the Operations Manager online Help.



# **Dataset storage space management**

---

The licensed provisioning application enables you to view space allocations for volumes, LUNs, and qtrees. You can also resize individual volumes or qtrees, and modify volume data and Snapshot copy space allocations in response to space-usage generated error or warning events.

The space allocation changes that you make apply only to the selected volume or qtree, not to any other volumes or qtrees in the dataset. You can specifically edit the space allocation for data and Snapshot copies as long as the space allocation remains compliant with the provisioning policy assigned to the associated dataset primary, backup, or mirror node.

## **Next topics**

[\*When to manually manage storage space for a dataset\*](#) on page 705

[\*How to view dataset storage space utilization\*](#) on page 706

[\*Overview of tasks for managing storage space\*](#) on page 706

[\*Space management resize options\*](#) on page 707

## **Related tasks**

[\*Viewing volume, LUN or qtree space allocation\*](#) on page 757

[\*Diagnosing volume or qtree space status\*](#) on page 759

[\*Resizing volume space\*](#) on page 761

[\*Resizing qtree space\*](#) on page 763

[\*Deleting Snapshot copies\*](#) on page 765

[\*Deleting a volume, LUN or qtree\*](#) on page 767

## **When to manually manage storage space for a dataset**

In most cases, you perform space management tasks on a volume, or qtree when a space-usage generated warning or error event alerts you to the fact that an individual storage container in one of your managed datasets has reached, or is close to reaching, its configured maximum capacity to hold new data.

At this point, in many cases, the simplest and most immediate remedy is to make more data space available for those individual volumes or qtrees.

**Note:** The only management task that you can perform on a LUN is to delete the LUN.

## How to view dataset storage space utilization

You can use the **Resource Pools** window Space breakout tab to see how much space each dataset is currently using, which is helpful for determining when a dataset needs to be migrated to a larger aggregate in another storage system.

The Space breakout tab lists the aggregates assigned to the resource pool that is selected in the **Resource Pools** window. When you select an aggregate, all the datasets in the aggregate and the percentage and amount of currently used space for each dataset are displayed.

Datasets that have a high percentage of utilization are good candidates for migration.

## Overview of tasks for managing storage space

If you have the provisioning license, you can perform different tasks to manage the storage space for a dataset.

### **Survey your volumes and qtrees.**

You can scan the tables on the Provisioning tab to pinpoint the volumes and qtrees that are approaching their data and Snapshot copy space limitation.

### **Diagnose your space management warning and error statuses.**

You can check the diagnosis of the volumes or qtrees whose space status is Warning or Error.

### **Resize your volume or qtree data and Snapshot space.**

In nodes containing volumes or qtrees, you can expand a volume to claim more uncommitted aggregate space or you can increase a qtree quota to claim more uncommitted volume space. You can also reallocate the space in a volume specifically reserved for Snapshot copies and specifically used for data.

### **Delete Snapshot copies.**

You can delete individual Snapshot copies in a volume to make more space available for data.

### **Delete storage containers.**

You can delete unneeded volumes and return the space that they used to the containing aggregate for reallocation. You can delete LUNs and qtrees and return the space they used to the containing volume for reallocation.

## Space management resize options

The provisioning application allows you as many as three options to resize or reallocate space on existing volumes. It also allows you to expand hard quotas on existing qtrees.

<b>Volume resize options</b>	Depending on the type of volume (NAS or SAN), the provisioning application enables you to modify one or more of the following parameters:
<b>Total volume size</b>	You can increase the total space allowed for the selected NAS or SAN volume within its containing aggregate. If you are not allowing space overcommitment, you are limited by the amount of space still available in the containing aggregate.
<b>Snap reserve %</b>	The percentage of space in the selected flexible volumes reserved for Snapshot copies. Snap reserve % is adjustable on NAS volumes. As you adjust the percentage up or down, the provisioning application displays the absolute allocation of Snapshot copy reserve space in the Snap Reserve field.
<b>Maximum size limit</b>	If the Autogrow property is enabled on a SAN or NAS volume, you can modify the Maximum size limit.

<b>Qtree resize option</b>	The provisioning application allows you to enlarge the hard quota for a qtree if the qtree is configured with a hard quota.
----------------------------	---

### Related tasks

[Resizing volume space](#) on page 761



# Dataset properties

---

You can use the following definitions when you configure or edit a dataset's properties and resources.

## General properties

The dataset properties menu enables you to modify the name, description, custom name prefix, ownership, and policy enforcement properties of an existing dataset. For an application dataset, the name of the application that created the dataset, the application version, and the server name running the application, also appear.

<b>Name</b>	The name of the dataset
<b>Description</b>	The description of the dataset
<b>Volume and qtree name prefix</b>	The prefix used to designate the volume or qtree in a dataset. The name prefix defaults to the dataset name or you can specify a custom prefix.
<b>Owner</b>	The name of the person responsible for this dataset
<b>Contact</b>	The e-mail address of each person who should be contacted about this dataset. You can separate multiple e-mail addresses with commas.
<b>Time Zone</b>	The time zone that protection policy schedules should use when timing protection events.
<b>IP address and netmask</b>	The IP address and netmask of the vFiler unit that will be provisioned when the first member of the dataset is provisioned. This property is active only for datasets that do not have a vFiler unit assigned.

## Related concepts

[Decisions to make before adding datasets](#) on page 711

## Related tasks

[Adding a dataset](#) on page 719



# Decisions to make before adding datasets

---

Before you use the **Add Dataset** wizard to create a dataset, you need to decide how you want to protect and provision the dataset.

## Next topics

*[Dataset protection decisions](#)* on page 711

*[Dataset provisioning decisions](#)* on page 714

*[Custom name prefixes for dataset volumes, qtrees, and Snapshot copies](#)* on page 716

## Related concepts

*[Effect of time zones on schedules](#)* on page 1049

*[What a protection policy is](#)* on page 847

*[Overview of resource pools](#)* on page 819

*[Protection policy node prerequisites](#)* on page 1051

*[What a provisioning policy is](#)* on page 848

## Related tasks

*[Adding a dataset](#)* on page 719

## Related references

*[Dataset properties](#)* on page 709

# Dataset protection decisions

Before you use the **Add Dataset** wizard to create a new dataset, and if you have the protection license, you need to decide how you want to protect the data and how you want to assign resources to contain backups or mirror copies.

**Dataset properties**

- When naming the dataset, is there a naming convention at your site to help administrators locate and identify datasets?

Dataset names can include the following characters:

a to z  
A to Z  
0 to 9  
. (period)  
\_ (underscore)  
- (hyphen)  
space

If you use any other characters when naming the dataset, they will not appear in the name.

- What is a good description of the dataset membership?  
Use a description so that someone unfamiliar with the dataset and the reasons supporting its creation understand its purpose.
- Will you include a volume and qtree name prefix so you can easily find all volumes and qtrees associated with the dataset?

Volume and qtree name prefixes can include the following characters:

a to z  
A to Z  
0 to 9  
. (period)  
\_ (underscore)  
- (hyphen)  
space

If you use any other characters, you will get an error message.

If you do not use a volume and qtree name prefix, the dataset name will be used.

- Who is the owner of the dataset?
- If an event on the dataset triggers an alarm, who should be contacted?  
You can provide an individual e-mail address for each person or a distribution list of people to be contacted.
- Should operations on the dataset be scheduled according to the local time zone for the data?

If so, you can specify a time zone in the wizard or use the default time zone, which is the system time zone used by the DataFabric Manager server.

- |                          |  |
|--------------------------|--|
| <b>Group membership</b>  | <ul style="list-style-type: none"> <li>• Do you need to create a collection of datasets and resource pools based on common characteristics, such as location, project, or owning organization?</li> <li>• Is there an existing group to which you want to add this dataset?</li> </ul>   |
| <b>Protection policy</b> | <ul style="list-style-type: none"> <li>• Which protection policy meets the requirements of the dataset?<br/>Review the policies listed on the <b>Protection Policies</b> window to see if any are suitable for your new dataset.</li> <li>• If no protection policy meets the requirements of your new dataset, is there a protection policy that would be suitable with minor modifications?<br/>If so, you can copy that protection policy to create a new policy you can modify as needed for the new dataset. If not, you can run the <b>Add Protection Policy</b> wizard to create a new policy for the dataset.</li> </ul> <p><b>Note:</b> You do not have to assign a policy to create a new dataset. You can assign a policy to the dataset later by running the <b>Dataset Policy Change</b> wizard.</p>  |
| <b>Resources</b>         | <p>Will you assign a resource pool or individual physical resources as destinations for your backups and mirror copies?</p> <p>You do not have to assign a resource pool or physical resources to a node to create a new dataset. However, the dataset will be nonconformant with its policy until resources are assigned to each node, because the licensed protection application cannot carry out the protection specified by the policy.</p> <p>If using a resource pool:</p> <ul style="list-style-type: none"> <li>• For each node in the dataset, which resource pool meets its provisioning requirements?<br/>For example, the resource pool you assign to a mirror node should contain physical resources that would all be acceptable destinations for mirror copies created of the dataset members.</li> <li>• If no resource pool meets the requirements of a node, you can create a new resource pool for each node at the <b>Resource Pools</b> window.</li> <li>• Verify that you have the appropriate software licenses on the storage you intend to use.</li> </ul> <p>If using individual resources:</p> <ul style="list-style-type: none"> <li>• If you prefer not to use resource pools for automatic provisioning, you can select individual physical resources as destinations for backups and mirror copies of your dataset.</li> <li>• Verify that you have the appropriate software licenses on the storage you intend to use.</li> </ul> |

## Related concepts

[What a protection policy is](#) on page 847

[Effect of time zones on schedules](#) on page 1049

[What a provisioning policy is](#) on page 848

# Dataset provisioning decisions

If you have the provisioning license, you must gather certain provisioning information before you use the **Add Dataset** wizard to create a new dataset. A dataset can have a single node or, if you assign a protection policy to it, a dataset can have a primary and one or more nonprimary nodes. When you first create a dataset, you configure the provisioning for the primary node only.

**Provisioning policy for** Do you want to assign a provisioning policy to manage the storage resources or do you want to manually assign resources?

**primary node**

- If you want to use a provisioning policy, have you already configured a policy that meets the requirements of the data in the dataset primary node?  
Review any existing policies that are listed in the **Provisioning Policies** window to see if any are suitable for your new dataset.
- If no current provisioning policy meets the requirements of your new dataset, is there a policy that would be suitable with minor modifications?  
If so, you can copy that policy and then modify it as needed. If no suitable provisioning policy exists, you can run the **Add Provisioning Policy** wizard to create a new policy.
- If you do not want to assign a provisioning policy at the time the dataset is created, you can assign a provisioning policy to the primary node later.

**Note:** After the dataset is added, whether or not it has a provisioning policy assigned, you can also provision new members for the dataset by using the **Provisioning** wizard.

- If you assign a NAS-based provisioning policy, do you want to enable CIFS or NFS export protocol access to the members of this dataset node?

You can enable one or both export protocols for all members of this node when you configure the dataset. You can also decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

However, you cannot enable CIFS export protocol access if the assigned provisioning policy is configured for the options "Guarantee space for dataset and Snapshot copies" (which is displayed in the **Provisioning Policies** window as "Guarantee space for dataset") and ""Guarantee initial size, allocate maximum size on-demand and allow automatic deletion of Snapshot copies" (which is displayed in the **Provisioning Policies** window as "Increase container size automatically").

- If you assign a SAN-based provisioning policy, do you want to enable FC or iSCSI export protocol access to the members of this dataset node?  
You can enable either protocol for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

**vFiler unit assignment and data migration capability**

Do you want to attach a vFiler unit to the dataset for data export?

If so, you can select an existing vFiler unit that is managed by the provisioning application or you can provide an IP address or network mask and the provisioning application will create a new vFiler unit. Attaching a vFiler unit enables automatic offline migration for the dataset. (Automatic offline migration requires that you shut down applications using the dataset before initiating the cutover step of the migration process.)

**Nonprimary dataset nodes**

After the dataset is created, if you have the protection license and the dataset has a secondary backup or mirror node, you can edit the dataset node to assign a provisioning policy to a nonprimary node.

- If you choose to associate a vFiler unit with a nonprimary node in a dataset, any volumes that are provisioned for that dataset must be associated with the vFiler unit. Therefore, when you view a list of the dataset volumes, only volumes that are owned by the vFiler unit are displayed.

**Note:** You cannot associate a vFiler unit with a nonprimary node unless it is a disaster recovery-capable nonprimary node.

- If you want to assign a NAS or SAN type provisioning policy instead of a secondary type policy to a nonprimary node, the dataset must be disaster recovery capable. This means that the dataset must also have a protection policy assigned that supports disaster recovery, and the nonprimary node must be the disaster recovery-capable node.

- The policy type (NAS or SAN) on the primary dataset node must match the policy type assigned to the nonprimary node.

- If you assign a NAS-based provisioning policy, do you want to enable CIFS or NFS export protocol access to the members of this dataset node?

You can enable one or both export protocols for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

- If you assign a SAN-based provisioning policy, do you want to enable FC or iSCSI export protocol access to the members of this dataset node?

You can enable either export protocol for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols

at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

**Note:** You should not use a version earlier than SnapDrive for Windows 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error, after which you must manually unmap the LUNs.

#### Related concepts

[Dataset migration overview](#) on page 769

[Overview of export protocol properties](#) on page 743

[What a provisioning policy is](#) on page 848

#### Related references

[Dataset migration requirements](#) on page 771

## Custom name prefixes for dataset volumes, qtrees, and Snapshot copies

When creating or editing a dataset, you can choose a custom name prefix for the volumes and qtrees in the dataset, and for the Snapshot copies. The name prefix helps you to easily locate volumes, qtrees, and Snapshot copies.

**Naming for primary nodes** For NAS provisioned datasets, you can specify a custom volume and qtree name prefix for all volumes included within the dataset. You can name the qtrees within those volumes at the time you create the qtree. If you do not use a volume and qtree name prefix, the dataset name is used.

The volume and qtree name prefix can include the following characters:

- a to z
- A to Z
- 0 to 9
- . (period)
- \_ (underscore)
- (hyphen)
- space

If you use other characters, you get an error message.

The volume and qtree name prefix is the volume name. Volume names are limited to 64 total characters, including underscores and suffixes. Suffixes are added if the volume name is a duplicate.

**Naming for nonprimary nodes**

For nonprimary nodes, you can specify a volume and qtree name prefix to apply to backups and mirrored copies. If your primary node is unavailable, you can locate the appropriate volumes and qtrees on a nonprimary node, using the naming prefix you specified when you created or edited your dataset.

The backup name consists of the volume and qtree name prefix and the backup type. Root qtrees being backed up on nonprimary nodes use the volume and qtree name prefix. However, qtrees created before the release of DataFabric Manager 3.8 will not use the volume and qtree name prefix.

The name of the mirrored copy includes the secondary volume and qtree name prefix, mirror type, primary host name, and the primary volume name.

For nodes that use the backup then mirror policy, the name includes the volume and qtree name prefix and the backup type (mirror).

If you do not specify a volume and qtree name prefix, the dataset name will be used.

For more information on the CLI commands necessary to access the nonprimary node, see the DataFabric Manager man pages.

**Naming Snapshot copies**

Snapshot copies have a date stamp prefix. The full name also includes the retention type, host name, volume name, and the qtrees included within the Snapshot copy. The name is shortened if there are too many qtrees in the Snapshot copy.

For more information on CLI commands for Snapshot copy naming, see the DataFabric Manager man pages.



# Adding a dataset

---

You can add a dataset to manage protection for data sharing the same protection requirements, or to manage provisioning for the dataset members.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
  - Provisioning policy for nonprimary dataset nodes
- If you plan to assign a policy, you need to be assigned a role that enables you to view policies.
- If you plan to assign a provisioning policy, you also need a role that enables you to attach the resource pools configured for the policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Datasets ▶ Overview**.
2. Click **Add** to start the **Add Dataset** wizard.

If you want to provision your node by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.

**Note:** If you receive a message that the maximum number of vFiler units has been reached, you must relinquish the migration capability for one or more datasets before you can configure an IP address and network mask that enables the migration capability for a dataset.

3. Complete the steps in the wizard to create a dataset.

If you have the protection license and you did not assign a protection policy to the dataset or assign resources to each destination node when creating the new dataset, the data is not yet protected.

If you have the provisioning license and you did not assign a provisioning policy to each of the dataset nodes, you will have to manually provision each node.

If you have the disaster recovery license and you did not assign a disaster recovery policy to the dataset, the data is not protected for disaster recovery.

#### **Related concepts**

*[Decisions to make before adding datasets](#)* on page 711

*[Effect of time zones on schedules](#)* on page 1049

#### **Related tasks**

*[Relinquishing migration capability of a dataset](#)* on page 797

*[How do I back up data?](#)* on page 589

*[Enabling disaster recovery protection](#)* on page 641

#### **Related references**

*[Dataset properties](#)* on page 709

*[Administrator roles and capabilities](#)* on page 1055

# Decisions to make before assigning or changing policies

---

Before you assign or change a policy, you need to gather information about the dataset and policies that you want the dataset to have.

You will need to gather the following information:

- |   |   |
|---|---|
| <b>Protection policy</b>                | <ul style="list-style-type: none"> <li>• Which protection policy meets the requirements of the dataset?<br/>Review the policies listed on the <b>Protection Policies</b> window to see if any is suitable for your new dataset.</li> <li>• If no protection policy meets the requirements of your new dataset, is there a protection policy that would be suitable with minor modifications?<br/>If so, you can copy that protection policy to create a new policy you can modify as needed for the new dataset. If no suitable protection policy exists, you can run the <b>Add Protection Policy</b> wizard to create a new policy for the dataset.</li> </ul>  |
| <b>Disaster recovery policy</b>         | <ul style="list-style-type: none"> <li>• What type of disaster recovery capable protection policy do you need?<br/>The licensed protection application provides disaster recovery capable protection policies that function similarly to the backup policies.<br/><br/><b>Note:</b> When you change a policy from backup to mirror or mirror to backup, the <b>Dataset Policy Change</b> wizard prompts you to establish a new baseline for the relationship. If you do, old data is retained, and the application makes a new copy of the entire dataset and transfers the active file system on the secondary. After reinitialization, you can manually delete the Snapshot copy.</li> <li>• If you are changing the protection policy to a disaster recovery policy, do you want to map the settings from a node in the old dataset to a node in the new dataset?<br/>You should copy the settings only if the path from the primary node is the same in the new policy as it was in the old policy.</li> <li>• Do you plan to use a failover script to shut down processes before the application invokes failover?<br/>If so, you need to define the path to a failover script.</li> </ul> |
| <b>Backup and mirror node resources</b> | <ul style="list-style-type: none"> <li>• If you are changing the protection policy for a dataset with backup and mirror nodes, do you want to use the same resource assignments that were used in the previous policy?<br/><br/>For example, if you have a dataset using the Mirror policy and you want to change to the Chain of two mirrors policy, you can choose to copy resources used for the single mirror node in the current policy to one of the two mirror nodes in the new</li> </ul>   |

policy. After you have copied resources from a node in the current policy, you cannot copy resources from that same node to any other node in the new policy.

- If you are assigning a policy for the first time or if you do not want to copy resources used in the current policy, is there a resource pool that meets the provisioning requirements of the dataset?

For example, the resource pool you assign to a mirror node should contain physical resources that would all be acceptable destinations for mirror copies created of the dataset members. If no resource pool meets the requirements of a nonprimary node, you can create a new resource pool for each backup and mirror node using the **Add Resource Pool** wizard.

- If you prefer to not use resource pools for automatic provisioning, which physical resources would be suitable as destinations for backups and mirror copies of the dataset?

**Note:** You do not have to assign a resource pool or physical resources to a destination node to assign or change a policy. However, the dataset will be nonconformant with its new policy until resources are assigned to each destination node, because the licensed application cannot carry out the protection specified by the policy.

#### Provisioning policy

- On which node do you want to assign or change the provisioning policy? If you have a protection license, your dataset might have a primary and one or more nonprimary nodes. You can assign the same provisioning policy to every node in the dataset, or you can assign a different provisioning policy to each node.
- Which provisioning policy meets the requirements of the dataset node? Review the policies listed on the **Provisioning Policies** window to see if any is suitable for the dataset node.

**Note:** If you are changing the provisioning policy, the policy type (NAS or SAN) on the primary dataset node must match the policy type assigned to the nonprimary node. If you want to assign a NAS or SAN type provisioning policy instead of a secondary type policy to a nonprimary node, the dataset must be disaster recovery capable. This means that it must also have a protection policy assigned that supports disaster recovery, and the node must be the disaster recovery capable node.

- If no provisioning policy meets the requirements of the dataset node, is there a provisioning policy that would be suitable with minor modifications? If so, you can copy that policy to create a new policy that you can modify as needed. If not, you can run the **Add Provisioning Policy** wizard to create a new policy for the dataset node.

#### Related concepts

[What a protection policy is](#) on page 847

*[Overview of resource pools](#)* on page 819

**Related tasks**

*[Assigning or changing a protection policy](#)* on page 725



# Assigning or changing a protection policy

---

You can assign a policy to a dataset or change the policy assigned to it. The policy specifies how the data is to be protected.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Determine which policy you want to assign to the dataset. You can review available protection policies on the **Protection Policies** window. If no policy meets the requirements of your new dataset, you can create a new policy or modify a copy of an existing policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can use this procedure after you have created a new dataset and want to assign a policy to it, or when you want to change the protection policy assigned to a dataset. You can also use this procedure to protect a dataset that is listed on the **Datasets** window.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select a dataset and click **Protection Policy** to start the **Dataset Policy Change** wizard.

**Note:** If you want to provision your nodes by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.

3. Complete the steps in the wizard.

## Related concepts

[\*Decisions to make before assigning or changing policies\*](#) on page 721

[\*What a protection policy is\*](#) on page 847

**Related tasks**

*How do I back up data?* on page 589

*Enabling disaster recovery protection* on page 641

**Related references**

*Administrator roles and capabilities* on page 1055

# Assigning or changing a provisioning policy

---

You can assign a provisioning policy to a dataset node or change the currently assigned provisioning policy assigned to a dataset node.

## Before you begin

- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
  - Provisioning policy for nonprimary dataset nodes
- Determine which policy you want to assign to the dataset node. You can review available provisioning policies listed in the **Provisioning Policies** window.  
If no provisioning policy meets the requirements of your dataset node, you can create and modify a copy of an existing policy or create a new policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to assign or change the provisioning policy and click **Edit**.
3. In the **Edit Dataset** window, click **Provisioning/Resource Pools** for the node to which you want to assign or change the provisioning policy.
4. On the Edit Provisioning and Resource Pools page, select a provisioning policy and click **Next**.
5. Continue to click **Next** until you reach the Preview Details page.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.
7. Close the **Edit Dataset** window.

## Related tasks

[Enabling deduplication on your dataset nodes](#) on page 809

## Related references

[Administrator roles and capabilities](#) on page 1055



## Decisions to make before provisioning a dataset

---

Before you use the **Provisioning** wizard to add a volume, qtree, or LUN to an existing primary dataset node, you need to gather the information required to complete the wizard.

**Prerequisites** Does the dataset that you are trying to provision have a resource pool assigned to it?

If not, you need to assign a resource pool before provisioning the node. You can check the resource pool assignment on the **Datasets** window Overview tab.

Does the dataset that you are trying to provision have a provisioning policy assigned to it?

If not, you need to assign a provisioning policy before provisioning the node. You can check the provisioning policy assignment on the **Datasets** window Overview tab.

**Note:** You are advised not to use SnapDrive for Windows versions earlier than 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error that requires the LUNs to be manually unmapped.

**Name** What is the export name of the volume or LUN that you want to provision?

The export name (NFS or CIFS protocol for NAS storage, or iSCSI or FCP protocol for SAN storage) is created with the name you specify.

**Description** What is the description of this provisioning request?

This information can be useful later: for example, if you want to track provisioning requests against IT helpdesk tickets.

**Size** What is the size of the qtree, volume or LUN?

- The minimum LUN size for Windows is 32 MB. For other operating systems it is 4 MB.
- The actual size that is provisioned is determined by the size that you specify in the wizard and by the provisioning policy that is assigned to the dataset node.
- **NAS storage example**

If you enter a maximum size of 20 GB in the wizard and the provisioning policy that is assigned to the dataset enables the Reserve space for Snapshot copies option, then the licensed application allocates 24 GB for the newly provisioned storage. If the provisioning policy does not enable the option for guaranteed space for data and Snapshot copies, the licensed application does not allocate space until the space is actually used. In this case, the total size refers only to the potential size that can be used, but the space is not guaranteed.

- SAN storage example

If you enter 50 GB for the data size and 50 GB for the maximum Snapshot copy size, and if the provisioning policy that is assigned to the dataset enables the option to guarantee space for data and Snapshot copies, the licensed application adds 50 GB for the overwrite reserve space and allocates a total of 150 GB for the volume.

What is the maximum space for Snapshot copies?

- If you are provisioning a LUN, what is the maximum amount of space in the volume that Snapshot copies can use?
- If you are provisioning a volume or qtree, what is the maximum amount of space in the resource pool that the volume or qtree can use?

When calculating the amount, include all of the LUNs, space reserves, and Snapshot copy space that the resource pool contains.

**Override exports** Which, if any, export protocol access do you want to enable for the volume, LUN, or qtree that you are provisioning?

This decision applies only if you have not already enabled an export protocol on the entire dataset into which you are provisioning the volume, LUN, or qtree.

- If you are provisioning NAS storage, do you want to enable NFS export access, CIFS export access, or both?
- If you are provisioning SAN storage, do you want to enable iSCSI export access or FC export access?

**Resource selection** How do you want to select the resource to provision into this dataset?

- Do you want the provisioning application to automatically provision a resource from the assigned resource pool?
- Do you want to manually select the resource from the assigned resource pool?

## Related concepts

[Overview of export protocol properties](#) on page 743

[How to select a specific aggregate or storage system for provisioning](#) on page 733

## Related tasks

[Provisioning resources for a primary dataset node](#) on page 731

# Provisioning resources for a primary dataset node

You can add a volume to the primary dataset node when you need to add more space to an existing dataset.

## Before you begin

- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Provisioning**.
2. Select the dataset that you want to provision.
3. Click **Provision** to start the **Provisioning** wizard.
4. On the Preview page, if any errors are displayed, click **Back** to return to previous pages in the wizard and correct the errors.  
The Preview page displays the results of a trial run of your provisioning request. Any potential errors are described and suggestions for resolving them are provided.
5. Complete the steps in the wizard and click **Next** in the Preview page to commit the provisioning request.

The provisioning request is sent to the server. The progress of the job is shown in the progress bar. When the job completes, the **Provisioning to the dataset** summary page on the wizard confirms the completion.

If you do not want to wait for the job to complete, you can close the wizard and processing continues in the background. You can monitor the progress of the provisioning job in the **Jobs** window.

When the job is done and the new volume is added, the licensed provisioning application compares the attributes of the volume to the provisioning policy assigned to the node, if any. If the new dataset member is out of conformance, the dataset status changes to Error and the conformance status for the dataset member changes to Nonconformant.

## Related concepts

[How to select a specific aggregate or storage system for provisioning](#) on page 733

*Decisions to make before provisioning a dataset* on page 729

**Related references**

*Administrator roles and capabilities* on page 1055

# How to select a specific aggregate or storage system for provisioning

---

When using the **Provisioning** wizard to add a new volume, qtree, or LUN container in the primary node of an existing dataset, you can provision that container with a specific aggregate or storage system from its assigned resource pool rather than having the **Provisioning** wizard automatically provision aggregates or storage systems from that resource pool.

When provisioning LUNs in a SAN environment, you might need to manually select a specific storage system from resource pool if the host that you are provisioning the LUNs for has access to only that specific storage system.

To provision a new volume, qtree, or LUN with a specific aggregate or storage system, you start the **Provisioning** wizard as you normally do.

When the **Provisioning** wizard displays the "Resource selection" panel, click **Manually select a resource from the attached resource pools** and select a specific storage system or aggregate from the resource pool trees display.

## Related concepts

[\*Decisions to make before provisioning a dataset\*](#) on page 729

## Related tasks

[\*Provisioning resources for a primary dataset node\*](#) on page 731



# Decisions to make before adding or changing resource assignments

---

Before you add or change the physical resources assigned to an existing dataset node, you need to gather the required information.

- For each node in the dataset, which resource pool meets its protection or provisioning requirements? For example, if you have the protection license, the resource pool you assign to a mirror node should contain physical resources that are appropriate for mirrored copies of the dataset. If you have the provisioning license, the resource pool you assign to a dataset node should contain physical resources that are appropriate and large enough for the provisioning needs of the data contained in the dataset node.
- What if there are no resource pools that meet the protection or provisioning requirements of the dataset node? If no resource pool meets the protection or provisioning requirements of a dataset node, you can use the **Resource Pools** window to create a new resource pool for each node.
- If you have the protection and disaster recovery license, can you choose not to use resource pools? You can select physical resources for the backup and mirror nodes of your dataset. If you choose to select storage outside of a resource pool, the licensed protection application does not create volumes but instead uses the volumes you select for that dataset node.
- If you have the provisioning or disaster recovery license, can you choose not to use resource pools? You can manually provision your dataset. If you choose to provision your dataset on storage outside of a resource pool, the licensed provisioning application does not create volumes but instead uses the volumes that you select for that dataset node.

**Note:** If you choose to associate a vFiler unit with a nonprimary node in a dataset, any volumes that are provisioned for that dataset must be associated with the vFiler unit. Therefore, when you view a list of the dataset volumes, only volumes that are owned by the vFiler are displayed.

## Related tasks

[Making the disaster recovery node the new primary data storage](#) on page 649



# Adding resources to a dataset

---

You can add physical resources to an existing dataset. Any protection, disaster recovery, and provisioning policy assigned to the dataset node is automatically extended to the newly added resources.

## Before you begin

- Have the resource information available that you need to complete this task:
  - Whether or not you want to use resource pools
  - The node's protection or provisioning requirements
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to add physical resources and click **Edit**.
3. In the **Properties** sheet, click **Physical Resources** for the node to which you want to add physical resources.

The Edit property sheet Overview page is the starting point for several different types of tasks. Each option on the menu starts an in-place property sheet or a wizard. Canceling or completing an option returns you to the Edit Overview page.

4. In the Edit Physical Resources page, select each new member from the Available Resources list and move it to the Resources in this Node list.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this Dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

You can filter the list of available resources by using the Group and Resource Type drop down menus. The Group filter allows you to view data that pertains to objects in the selected group. The Resource Type filter allows you to sort by either hosts, aggregates, qtrees, or volumes. You will be able to see the resources for which you have permissions.

5. Click **Next**.

The licensed application generates a report detailing the impact of the changes to the dataset.

6. After you are satisfied with the preview results, click **Next** to apply your changes, then click **Finish** to return to the property sheet Overview page.

The licensed application updates the physical resources of the dataset.

**Related references**

*Administrator roles and capabilities* on page 1055

# Changing dataset node resource assignments

---

If the protection, failover, or provisioning requirements of your dataset change, you can add physical resources to a dataset node or change the resources currently assigned to a dataset node.

## Before you begin

- Have the resource information available that you need to complete this task:
  - Whether or not you want to use resource pools
  - The node's protection or provisioning requirements
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to change physical resources and click **Edit**.
3. In the **Edit Dataset** window, click **Physical Resources** for the node to which you want to change the physical resources.
4. In the Edit Physical Resources page, add a new physical resource by selecting a resource from the Available Resources list and moving it to the Resources in this Node list.

Remove a resource by selecting a resource from the Resources in this Node list and moving it to the Available Resources list.

You can filter the list of available resources by using the Group and Resource Type drop down menus. The Group filter allows you to view data that pertains to objects in the selected group. The Resource Type filter allows you to sort by either hosts, aggregates, qtrees, or volumes. You will be able to see the resources for which you have permissions.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

5. Click **Next**.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.

If no resources were previously assigned to the dataset node, the dotted outline in the graph area of the **Datasets** window Overview tab is replaced by an icon representing assigned storage.

**Related concepts**

[\*What groups are\*](#) on page 1047

**Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Removing resources from a dataset

---

You can remove physical resources from an existing dataset when you no longer want to protect, fail over, or provision its data using the assigned policy.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset from which you want to remove physical resources and click **Edit**.
3. In the **Edit Dataset** window, click **Physical Resources** for the node from which you want to remove physical resources.
4. In the Edit Physical Resources page, select each resource you want to remove from the list and move it to the Available Resources list.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this Dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

5. Click **Next**.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.
7. Close the **Edit Dataset** window.

The licensed application removes the physical resources from the dataset.

## Related references

[Administrator roles and capabilities](#) on page 1055



## Overview of export protocol properties

---

If you have the provisioning license installed, you can configure access for clients using NFS, CIFS, iSCSI, or Fibre Channel (FC) protocols when you create or reconfigure the primary, backup, or mirror nodes in your datasets or when you provision new volumes, LUNs, or qtrees as members into your datasets.

**CIFS access** To configure support for CIFS client access to the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The Windows domain of the target nodes in this dataset
- Specific permissions (full control, no access, or read and change) for specific users to access the nodes in this dataset

**NFS access** To configure support for NFS client access to the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node in the dataset and specify the following:

- Default permissions (Read only, read write, or root access) for all NFS hosts to access the selected node in this dataset
- Specific permissions for specific NFS hosts to access the selected node in this dataset
- The NFS security protocol (Kerberos v5 Integrity, Kerberos v5, Kerberos v5 Privacy, UNIX style, or None) that you want enforced
- A default mapping for anonymous users to the selected node
- Whether or not to enable superuser ID access to the selected node in this dataset

**Fibre Channel access** To configure support for FC client access to the SAN-based volumes, or LUNs in the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
- The World Wide Port Names for the FC nodes, if the accessing host does not have NetApp Host Agent installed

**iSCSI access** To configure support for FC client access to the SAN-based volumes or LUNs in the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
- The initiator ID for the iSCSI nodes, if the accessing host does not have a NetApp Host Agent installed

#### **Related concepts**

[\*About NFS, CIFS, iSCSI, or FC protocol access\*](#) on page 699

[\*Decisions to make before provisioning a dataset\*](#) on page 729

[\*Dataset provisioning decisions\*](#) on page 714

#### **Related tasks**

[\*Displaying export properties for a specific dataset member\*](#) on page 417

# Configuring dataset nodes for CIFS protocol access

You can configure Windows client CIFS access to all NAS volumes or qtrees contained in a dataset's primary, backup, or mirror node if the dataset is configured to support CIFS access.

## Before you begin

- Confirm that the dataset node on which you want to enable CIFS access is assigned a NAS-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset you want to configure and click **Edit**.
3. In the **Edit Dataset** window, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify CIFS access.

If no provisioning policy has been assigned to this dataset, specify a NAS-type provisioning policy. The licensed application displays the provisioning policy assigned to the dataset node, and if that policy is a NAS-type policy, displays a CIFS Settings bar.
4. If the CIFS settings are not displayed, click the down arrow button on the CIFS Export Settings bar to expand the display.
5. Configure the CIFS settings. If CIFS is turned off, click **Turn CIFS On** to enable the settings.
6. Modify any other CIFS protocol or resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, and click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Configuring dataset nodes for NFS protocol access

You can configure NFS host access to all NAS volumes or qtrees contained in a dataset's primary, backup, or mirror node if the dataset is configured to support NFS access.

## Before you begin

- Confirm that the dataset node on which you want to enable NFS access is assigned a NAS-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual volumes or qtrees as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify NFS access.  
If no provisioning policy is assigned to this dataset, specify a NAS-type provisioning policy.  
The licensed application displays the provisioning policy assigned to the dataset node, and, if that policy is a NAS-type policy, displays an NFS Settings bar.
4. If the NFS settings are not displayed, click the down arrow button on the NFS Export Settings bar to expand the display.
5. Configure the NFS settings. If NFS is turned off, click **Turn NFS On** to enable the settings.
6. Modify any other NFS protocol or resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.  
If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Configuring dataset nodes for FC protocol access

You can configure Fibre Channel protocol (FC) client access to all SAN LUNs contained in a dataset's primary, backup, or mirror node if the dataset is configured to support FC access.

## Before you begin

- Confirm that the dataset node on which you want to enable FC access is assigned a SAN-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Note:

- FC is *not* supported on vFiler units
- If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify FC access.

If no provisioning policy has been assigned to this dataset, specify a SAN-type provisioning policy.

The licensed application displays the provisioning policy assigned to the dataset node. If that policy is a SAN-type policy, it displays an FCP Settings bar.

4. If the FC settings are not displayed, click the down arrow button on the FCP Export Settings bar to expand the display.
5. Configure the FC settings. If FC is turned off, click **Turn FCP On** to enable the settings.  
If iSCSI is turned on, it is automatically turned off when you click Turn FCP on.
6. Modify any other protocol and resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.

9. Close the **Edit Dataset** window.

**Related concepts**

*[About NFS, CIFS, iSCSI, or FC protocol access](#)* on page 699

**Related references**

*[Administrator roles and capabilities](#)* on page 1055

# Configuring dataset nodes for iSCSI protocol access

You can configure iSCSI client access to all SAN LUNs contained in a dataset's primary, backup, or mirror node if the dataset is configured to support iSCSI access.

## Before you begin

- Confirm that the dataset node on which you want to enable iSCSI access is assigned a SAN-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify iSCSI access.

If no provisioning policy has been assigned to this dataset, specify a SAN-type provisioning policy. The licensed application displays the provisioning policy assigned to the dataset node. If that policy is a SAN-type policy, it displays an iSCSI Settings bar.
4. If the iSCSI settings are not displayed, click the down arrow button on the iSCSI Export Settings bar to expand the display.
5. Configure the iSCSI settings. If iSCSI is turned off, click **Turn iSCSI On** to enable the settings. If FCP is turned on, it is automatically turned off when you click **Turn iSCSI on**.
6. Modify any other resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Editing dataset general properties

You can edit the general properties of an existing dataset, as well as the dataset's physical resources, provisioning policy, export settings, and resource pools.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset that you want to modify then click **Edit**.
3. In the **Edit Dataset** window, use the menu to click the property that you want to modify.

If you want to modify...	Then...
The name, description, or volume and qtree name prefix of the dataset	Click <b>General Properties</b> .
The physical resources of the dataset's primary data	Under Primary data, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's primary data	Under Primary data, click <b>Provisioning/Resource Pools</b> .
The physical resources of the dataset's backup data	Under Backup, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's backup data	Under Backup, click <b>Provisioning/Resource Pools</b> .
The physical resources of the dataset's mirror data	Under Mirror, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's mirror data	Under Mirror, click <b>Provisioning/Resource Pools</b> .

4. Modify the dataset properties as needed, then click **Finish** to return to the **Edit Dataset** window.

The application saves your changes. If you modified the dataset name, the new name is displayed on the **Datasets** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a dataset

---

You can delete a dataset if you want to stop protection or disaster recovery for all of its members and stop conformance checking against its assigned protection and disaster recovery policies.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset that you want to delete and click **Delete**.

The Delete Dataset dialog box opens, requesting that you confirm the deletion.

**Note:** When you delete a dataset, the physical resources that compose the dataset are not deleted.

3. Click **Yes** to confirm the delete request or **No** to cancel the request and close the dialog box.

The licensed application removes the dataset from the list in the **Datasets** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Overview of managing protected data

---

After you configure a dataset, you can monitor its status and its protection policy for possible errors, back up its content on-demand, suspend and resume protection for it, and initiate restore operations to access backed-up data. You can perform these management tasks using the **Datasets** window Overview tab.

## Monitoring dataset status

The licensed protection application provides the following three status types with which you can monitor your datasets:

<b>Protection Status</b>	Indicates whether the licensed application is protecting the data and is successfully creating backup copies, or whether there is an error while protecting the data.
<b>Conformance Status</b>	Indicates whether the dataset is properly configured and conforms to its protection policy.
<b>Resource Status</b>	Indicates whether the storage systems assigned to a dataset are functioning properly.

## Monitoring backup and mirror relationships

You can monitor backup or mirror relationships only if they are assigned to a dataset that is governed by a protection policy. For example, you can monitor the lag status of each relationship or monitor that backups are being created as scheduled.

## Backing up datasets on-demand

If you want to create copies of your data at any time other than as scheduled, you can back up the data on-demand and specify a duration for which the copy must be retained.

## Suspending and resuming protection of data

You can suspend data protection if you want to stop protecting a particular dataset but want to preserve its backup relationship. While data protection is suspended, the licensed application does not create new backup copies or mirror data.

Resuming data protection allows the licensed application to continue generating backup copies and mirroring data.

## Restoring data

The licensed application tracks where it made copies of the original primary data and enables you to restore the data from any of its copies. You can restore files contained in volumes, qtrees, and Open Systems SnapVault directories that are members of a dataset.

### Next topics

[\*Description of dataset protection status\*](#) on page 394

[\*Description of dataset conformance status\*](#) on page 395

[\*Description of dataset resource status\*](#) on page 395

## Description of dataset protection status

A dataset is protected only if the secondary storage system specified in the protection relationship is successfully backing up data, and if the copies of the data can be restored. You can monitor dataset status using the **Datasets** window Overview tab.

Ensure that you regularly monitor a dataset's protection, because the licensed protection application cannot sufficiently protect the dataset under the following conditions:

- If a secondary storage system runs out of storage space necessary to meet the retention duration required by the protection policy
- If the lag thresholds specified by the policy are exceeded

The following list defines protection status values and their descriptions:

<b>Job Failure</b>	A dataset error occurred during a data protection operation.
<b>Lag Warning</b>	The dataset is nearing the policy's lag threshold.
<b>Lag Error</b>	The policy's protection lag exceeded the configured threshold.
<b>No Protection Policy</b>	No protection policy has been assigned to the dataset.
<b>Protected</b>	The dataset is being protected according to its assigned protection policy.
<b>Protection Suspended</b>	The dataset administrator has requested that all scheduled backups be suspended until the administrator requests that they are resumed.
<b>Uninitialized</b>	The dataset does not have any backups that can be restored.

## Description of dataset conformance status

The dataset conformance status indicates whether a dataset is configured according to its protection policy. To be in conformance, all secondary and tertiary storage systems that are part of the backup relationship must be successfully provisioned and the provisioned volumes must match the requirements of the primary data. You can monitor dataset status using the **Datasets** window.

The licensed protection application regularly checks a dataset for conformance. If it detects changes in the dataset's membership or policy definition, the application does one of three things:

- Automatically performs corrective steps to bring a dataset back into conformance
- Presents you with a list of actions for your approval prior to correction
- Lists conditions that it cannot resolve

You can view these actions and approve them in the Conformance Details dialog box.

A dataset might be nonconformant because there are no available resources from which to provision the storage or because the licensed protection application does not have the necessary credentials to provision the storage resources.

The following list describes dataset conformance values:

<b>Conformant</b>	The dataset is conformant with its protection policy.
<b>Conforming</b>	The dataset is not in conformance with its protection policy. the licensed protection application is performing actions to bring the dataset into conformance.
<b>Nonconformant</b>	The licensed protection application cannot bring the dataset into conformance with its protection policy and might require your approval or intervention to complete this task.

## Description of dataset resource status

The dataset resource status indicates the event status for all resource objects that are assigned to the dataset. The resources include those that are members of the secondary and tertiary storage systems. If, for example, a tertiary member's status is critical, the dataset's resource status also is displayed as critical.

You can monitor dataset status using the **Datasets** window. You can troubleshoot the resource objects using the **Notifications > Events**.

The following list describes resource status values:

<b>Normal</b>	The resource is operating within the desired thresholds.
---------------	--

<b>Information</b>	A normal resource event occurred. No action is required.
<b>Warning</b>	The resource experienced an occurrence that you should be aware of. This event severity does not cause service disruption, and corrective action might not be required.
<b>Error</b>	The resource is still performing, but corrective action is required to avoid service disruption.
<b>Critical</b>	A problem occurred that might lead to service disruption if you do not take immediate corrective action.
<b>Emergency</b>	The resource unexpectedly stopped working and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.

# How to evaluate dataset conformance to policy

---

The licensed protection application periodically checks that the dataset conforms to its *data protection policy*. If either the dataset membership or policy changes, the licensed protection application either tries to bring the dataset back into conformance or notifies the administrator that the dataset *conformance* status changed to nonconformant.

You can view the Conformance Results from the **Datasets** window by clicking  next to Conformance in the Status area.

## Next topics

[Why datasets fail to conform to policy](#) on page 397

[How the protection application monitors dataset conformance](#) on page 397

[Dataset conformance conditions](#) on page 399

## Why datasets fail to conform to policy

A dataset must meet several conditions to be conformant to its assigned policy.

A dataset is conformant to its policy when it meets the following conditions:

- Its member storage systems are properly configured.
- Its assigned secondary storage system is provisioned and has enough backup space.
- Its protection policy includes all necessary relationships to enforce data backups or mirror copies.

Following are some of the common reasons datasets fail to conform to their protection policy:

- Dataset protection policy definitions changed.
- Dataset membership changed.
- Volumes or qtrees were created or deleted at the storage system (external to the licensed protection application).

## How the protection application monitors dataset conformance

The licensed protection application's *conformance monitor* regularly checks the DataFabric Manager database for configuration information to determine if a dataset is in conformance with its assigned policy.

Conformance status is determined based on data gathered from SNMP queries by system monitors. The monitors update the DataFabric Manager database at scheduled intervals. The conformance monitor queries the DataFabric Manager database for the information that is then displayed in NetApp Management Console. As a result, the information displayed by the conformance checker is not real-time data. This can result in the conformance checker results being temporarily out of date with actual changes to a storage system or configuration.

Should a dataset be nonconformant, you can view the conformance details from the **Datasets** window by selecting an item in the dataset list then clicking next to Conformance in the Status area. This opens the Conformance Results window, that shows the results of the last conformance run on the selected dataset. The results provide a description of any problems found during the last conformance run and suggestions for resolving the problems. Depending on the results shown, you can then either make changes manually to your system configuration or click Conform Now to allow the protection application to automatically make changes in an attempt to bring the dataset into conformance.

When you click Conform Now, you give the protection application full control to do whatever it can to bring everything into conformance for the selected dataset. This could include initiating a rebaseline of your data, which might require significant time and bandwidth. As a result, if you would not want a rebaseline to occur, you should try manual corrections to your system to resolve conformance issues before you choose to use the Conform Now option.

After making manual corrections to your system, you can return to the Conformance Results window and click the Preview Conformance button to see if any changes made to the system have brought the dataset into conformance with the policy assigned to it. Preview Conformance initiates a new check on the dataset but does not execute a conformance run. The results of the check reflect the latest system updates that have been identified by the monitors and captured in the DataFabric Manager database. Therefore, the information displayed in the Conformance Results window might not reflect recent changes made to a storage system or configuration and could be outdated by a few minutes or a few hours, depending on the changes made and the scanning interval for each monitor.

You can view a list of monitor intervals by using the command `dfm option list | grep Interval`. Following are some common monitoring actions, the default update intervals, and the associated monitors:

<b>Discover new hosts</b>	Default interval: 15 minutes Monitor: discover
<b>Update sizes for aggregates, volumes, and free or used space</b>	Default interval: 30 minutes Monitor: dfmon
<b>Find new disks, aggregates, volumes, qtrees</b>	Default interval: 15 minutes Monitors: fsmon, diskmon
<b>Find vFiler units</b>	Default interval: 1 hour Monitor: vfiler

**SnapMirror, SnapVault, and OSSV directory discovery** Default interval: 30 minutes  
 Monitor: relationships

**Update license capabilities on storage systems** Default interval: 4 hours  
 Monitor: license

## Dataset conformance conditions

The licensed protection application displays a dataset's conformance status in the **Datasets** window Overview tab. If the dataset is nonconformant, there are several ways in which the dataset can be brought back into conformance.

You can view the Conformance Results from the **Datasets** window by clicking  next to Conformance in the Status area.

When the conformance monitor detects a change in the dataset's membership or policy definition, the conformance monitor does one of three things:

- Automatically performs corrective steps to bring a dataset back into conformance
- Presents you with a list of actions for your approval prior to correction
- Lists conditions that it cannot resolve

### Conditions the monitor can resolve

The following list describes some of the conditions that the conformance monitor can detect, the actions it can take to bring the dataset back into conformance with its policy, and whether those actions are automatic or they require your approval for completion.

- The licensed protection application provisions a destination volume but the aggregate in which the volume is contained is no longer a member of the assigned resource pool.

**Corrective action:** The licensed protection application creates a new volume and moves the relationship to it.

Does the action require your approval? Yes

**Corrective action:** The licensed protection application moves the relationship to an existing volume.

Does the action require your approval? Yes

- The licensed protection application provisions a destination volume but the aggregate in which the volume is contained is no longer a member of the assigned resource pool.

- Corrective action:** The licensed protection application creates a new volume and moves the relationship to it.
- Does the action require your approval? Yes
- Corrective action:** The licensed protection application moves the relationship to an existing volume.
- Does the action require your approval? Yes
- The destination volume does not have enough backup space or it is over its "nearly full" threshold.
- Corrective action:** The licensed protection application expands the volume in an aggregate that is a member of the resource pool.
- Does the action require your approval? No
- Corrective action:** The licensed protection application provisions the volume and migrates the physical relationship to a new destination volume.
- Does the action require your approval? Yes
- The destination volume contains expired backup versions.
- Corrective action:** The licensed protection application deletes the backup versions. The application also deletes the copies of the data if those copies do not contain other backup versions.
- Does the action require your approval? No
- Policy calls for the source data to be mirrored but the source volume is not protected in a mirror relationship.
- Corrective action:** The licensed protection application creates a new relationship and performs a baseline transfer of the data. A baseline transfer is defined as an initial backup (also known as a level-0 backup) of a primary volume to a secondary volume in which the entire contents of the primary volume are transferred.
- Does the action require your approval? No
- Policy calls for the source data to be backed up but the source qtree is not protected in a backup relationship.
- Corrective action:** The licensed protection application creates a new relationship and performs a baseline transfer of the data.
- Does the action require your approval? No
- The primary volume has extra mirror relationships.
- Corrective action:** The licensed protection application deletes the extra relationships.

Does the action require your approval? No

- The primary qtree has extra backup relationships.

**Corrective action:** The licensed protection application deletes the extra relationships.

Does the action require your approval? No

### Conditions the monitor cannot resolve

The following list describes some of the conditions that the conformance monitor can detect but cannot resolve. These conditions require manual intervention from an administrator to bring the dataset back into conformance with its policy.

- An imported relationship has been detected in which the secondary volume exceeds the volFullThreshold.

**Corrective action:** You must manually increase the secondary volume size. The conformance monitor cannot resolve this condition.

- A dataset's assigned secondary resources do not offer appropriate backup space.

**Corrective action:** You must reconfigure the resource pool membership so that the licensed protection application can successfully continue data protection.

- The application does not have the appropriate credentials to access the assigned resources.

**Corrective action:** You must provide the credentials for access to the hosts or storage systems.



# Monitoring dataset status

---

You can monitor the status of your datasets and their protection policies for possible errors.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Datasets ▶ Overview**.
2. (Optional) You can customize the **Datasets** window Overview tab in any of the following ways:
  - Select a dataset to see the configured policy for that dataset and the details about each component in the policy.
  - Click  in a column header to control which dataset entries you want displayed. The color of the column header changes to indicate that you are filtering the entries in that column. Some column filters display a drop-down list to select from and other column filters display a search field in which you can enter text to select.
  - Click the sort arrows in a column header to change the sort order of the entries in that column.
  - Click  in the upper-right corner of the list to select which columns are displayed.
  - Drag the bottom of the dataset list area up or down to resize that area.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Monitoring backup and mirror relationships

---

You can monitor backup or mirror relationships that are governed by a protection policy that is assigned to a dataset. For example, you can monitor the lag status of each relationship or monitor that backups are being created as scheduled.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. (Optional) You can customize the **Datasets** window Overview tab in any of the following ways:
  - Select a dataset to see the configured policy for that dataset and the details about each component in the policy.
  - Click  in a column header to control which dataset entries you want displayed. The color of the column header changes to indicate that you are filtering the entries in that column. Some column filters display a drop-down list to select from and other column filters display a search field in which you can enter text to select.
  - Click the sort arrows in a column header to change the sort order of the entries in that column.
  - Click  in the upper-right corner of the list to select which columns are displayed.
  - Drag the bottom of the dataset list area up or down to resize that area.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Backing up datasets on-demand

---

If you want to obtain copies of your data at any time other than as scheduled, you can back up datasets on-demand and specify a duration during which the copy must be retained.

## Before you begin

- The dataset must have a protection policy assigned.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
  2. From the list of datasets in the **Datasets** window, select the dataset that you want to back up and click **Protect Now**.
  3. In the Protect Now dialog box, type a description for the on-demand backup.
  4. Also in the Protect Now dialog box, specify the schedule type (hourly, daily, weekly, or monthly) that specifies the duration that you want the backup copy retained.
- Note:** If a throttle schedule is applied to the dataset, it will also apply to the on-demand backup.
5. Click **OK**.

The licensed protection application starts a backup job to protect the data and directs you to the **Jobs** window from which you can track the job's progress.

If successful, the licensed protection application creates backup copies for all nodes governed by the policy.

## After you finish

You can restore the backed-up data by clicking **Restore** to start the **Restore** wizard.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Suspending protection of datasets

---

You can stop data protection temporarily without deleting the dataset. If the dataset's primary node is also assigned a provisioning policy, you can either suspend just the scheduled protection operations and keep the provisioning policy's conformance checking in place, or you can suspend both the protection operations and the conformance checking.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You might want to stop protection and conformance checking to perform maintenance on volumes used as destinations for backups or mirror copies.

**Note:** When you suspend services on application datasets, the external application continues to perform local backups as scheduled.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset and click **Suspend**.

The application requests confirmation that you want to suspend conformance checks on the dataset.

3. Click **Yes**.

The Details area of the **Datasets** window shows that the conformance status of the dataset has changed.

All scheduled backups and provisioning are cancelled until service is resumed.

**Note:** If you suspend protection for a dataset and the lag time exceeds the threshold defined for the dataset, no lag threshold event is generated until protection is resumed. After you resume protection for the dataset, the licensed protection application generates the backlog of lag threshold events that would have been generated had protection been in effect and triggers any applicable alarms.

## After you finish

You can resume data protection from the **Datasets** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Suspending data protection for backup volume maintenance

---

You might want to conduct periodic maintenance services on a secondary volume that is part of a backup or mirror relationship. Prior to taking the backup volume offline, you must first suspend protection of the dataset to which the volume belongs to ensure that the licensed protection application does not initiate a new backup or mirror relationship for the primary data.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the **Datasets** window, select the dataset to which the backup volume belongs and click **Suspend**.
3. In the Suspend dataset dialog box, click **Yes**.

The licensed protection application suspends dataset protection. While the application suspends protection, it displays a Protection Suspended status for the dataset and you can safely take the backup volume offline for maintenance services.

4. After you bring the storage system backup volume back online, you must wait for the DataFabric Manager server to recognize that the volume is back online. You can check the backup volume status using Operations Manager.
5. After the backup volume is recognized by DataFabric Manager, select from the list of datasets the one for which protection is suspended and click **Resume**.

The licensed protection application resumes data protection.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Resuming protection of datasets

---

You can cause the licensed protection application to resume protecting datasets and continue generating backup copies and mirroring data on schedule.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the **Datasets** window, select the dataset for which protection is suspended and click **Resume**.

The licensed protection application resumes data protection.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Displaying export and mapping information for all members of a dataset node

---

You can display export protocol and physical resource mapping information for all members of a selected dataset node.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.

The provisioning application displays the datasets included in your view.

2. Select the dataset that contains the dataset node whose export and physical resource mapping you want to display.

The provisioning application displays the nodes of the selected dataset.

3. Select the dataset node whose export and physical resource mapping you want to display.

The provisioning application displays overview status information for the selected node.

4. Locate the Exports parameter and click  next to it.

The provisioning application displays the Exports Mapping list which lists the path export protocol and physical resource path for every dataset member contained on the selected node.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Displaying export properties for a specific dataset member

---

You can display detailed export protocol properties for a selected dataset member. The export properties displayed are the same as those you configured for either the individual dataset member or as those you configured for the containing dataset node.

## Before you begin

- Know the dataset location of the dataset member whose export protocol information you want to display.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Provisioning**.

The provisioning application displays the names of the datasets that you have access to in data column of the top table.

2. Select the dataset that contains the dataset member whose export protocol properties you want to review.

The provisioning application displays the names of the members of the selected dataset in the storage column.

3. Select the dataset member that has the export protocol properties that you want to display and click the Exports tab.

The provisioning application displays the export protocol properties for the selected dataset member.

**Note:** The export properties displayed are the same as either those you configured for the individual dataset member or those you configured for the containing dataset node.

## Related concepts

[Overview of export protocol properties](#) on page 743

## Related references

[Administrator roles and capabilities](#) on page 1055



# Overview of restoring data

---

The licensed protection application tracks where it has made copies of the original primary data and enables you to restore the data from any of its copies.

Using the licensed protection application, you can restore files contained in volumes, qtrees, vFiler unit directories, Open Systems SnapVault directories, and virtual machines (VMs) that are members of a dataset.

You can choose to restore data to the following locations:

- The data's original location.

**Note:** If you are restoring a LUN, the following points apply:

- If the protection application is not configured to support non-disruptive LUN restore, the LUN in the destination location must be offline before you start the restore operation.
- If the protection application is configured to support non-disruptive LUN restore, the LUN in the destination does not have to be offline unless it is owned by a vFiler unit.
- If the destination LUN is owned by a vFiler unit, non-disruptive LUN restore is not supported.

- A new location.

If you restore data to a new location that is not contained in a dataset, then your restored data is not protected in its new location. To protect the restored data, add it to a dataset.

You can initiate a restore operation by invoking the **Restore** wizard from the Overview tab in the **Datasets** window. After you complete a restore request, you can use the **Jobs** window to view the progress of the restore job and also monitor it for possible errors. You can also enable the protection application to update you on job progress through desktop messages.

## Special restores for virtual machines only

If you are restoring a virtual machine, you have three types, rather than two types of restore location options.

- The virtual machine's original location

The virtual machine is restored and installed on its original location, through its original Open Systems SnapVault host on its original ESX server.

- A new location

The virtual machine image and data is stored as files in another location. If read by a virtual machine reader, it can run as an active virtual machine.

- Another ESX server

If the original Open Systems SnapVault host does not exist anymore, you can restore the virtual machine to the original location through any other Open Systems SnapVault host on an ESX server which can access the data store.

## **Supported data restore operations**

- Restore data from a local backup copy
- Restore data from a remote backup copy
- Restore data from the backup of a mirror
- Restore data from the mirror of a backup
- Restore data to an Open Systems SnapVault host
- For virtual machines, restore data to any location

## **File overwrite and out-of-space warnings for file-level restore**

Before executing a file-level restore from a storage system backup you can enable the protection application to warn about file overwrite or out-of-space conditions during restore.

- File overwrite warnings are issued if a file is detected in the target container with a name that matches a backup file that was selected for restore.

**Note:** In most cases, if you are restoring a file from a backup to a destination location, an overwrite of the file in the destination location by its backup version is what is intended. Nevertheless, the protection application will warn you to prevent the accidental overwrite of the destination file version.
- Out-of-space warnings are issued if the target container does not have enough free space to accommodate restore of a selected file.

### **Note:**

- The protection application will not issue file overwrite or out-of-space warnings for volume-level restores, qtree-level restores, folder-level restores, restores from Open System SnapVault backups, or restores from ESX server backups.
- File overwrite warnings are not issued if the restore target storage system is running Data ONTAP 7.2. x or earlier.
- Out-of-space warnings are not issued if the restore source storage system is running Data ONTAP 7.1.x or earlier.

## **Next topics**

[Restore guidelines](#) on page 421

[The restore\\_symboltable file](#) on page 421

## Restore guidelines

Review these guidelines prior to restoring data using the licensed protection application.

- The licensed protection application restores data components as small as single files and as large as qtree units. If you want to restore a complete volume, you must restore all its qtree members.
- When restoring data to an Open Systems SnapVault host, the licensed protection application overwrites the existing destination Open Systems SnapVault directories and their files.
- In an Open Systems SnapVault relationship, if the secondary storage is in a different domain than its Open Systems SnapVault host, the `/etc/hosts` files must include FQDN-IP mapping.

## The `restore_symboltable` file

When the licensed protection application restores copies of the primary data, Data ONTAP adds a `restore_symboltable` file in the destination directory. After you successfully restore the desired data, you can delete this file from the directory.

For more information about the `restore_symboltable` file, see the Data ONTAP man pages.



# Restoring backed-up data to a new location

---

You can restore backed-up data to a new location if you want to preserve the current content of a dataset. After you restore the backed-up files, you can decide whether you want to overwrite the existing data with the backed-up files.

## Before you begin

- Before restoring backed up data to a new location, ensure that the following conditions are true:
  - You know the backup version that you want to restore.
  - You know which volumes, qtrees, directories, files, or Open System SnapVault directories you want to restore.
  - You know the new volume or qtree location to which you want to restore the files.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that includes the backup files that you want to restore.
3. Click **Restore** to start the **Restore** wizard.

The wizard displays the **Backup Files** window.

4. If you want the **Restore** wizard to warn of file overwrite or out-of-space conditions during a file-level restore, select **Warn about overwrite and out-of-space conditions on the destination**.

**Note:** This option enables warnings only for file-level restores from storage system backups.

The **Restore** wizard does not issue file overwrite or out-of-space warnings for volume-level restores, qtree-level restores, folder-level restores, restores from Open Systems SnapVault backups, or restores from ESX server backups.

5. From the list of backups in the left pane, select the backup copies that you want to restore.

All copies are displayed by their backup dates and their dataset descriptions. All backup files that belong to the restored data are displayed in the right pane. Currently unavailable copies are marked as such.

6. Select the volume, qtrees, directories and files contained in the backup copies that you want to restore and click **Next**.

You can select multiple volumes, qtrees, directories or files simultaneously.

7. In the **Restore Preferences** window, click **Choose a location** to restore the files in a new location and click **Next**. (The list shows only volumes that are online.)
8. In the **Restore Path** window, either select the volume or qtree in which you want to restore the files or type the restore path in the Restore path field, then click **Next**.

The volume to which you are restoring the backup files must contain a directory.

The **Restore** wizard executes a dry run of your request and tests for warning conditions.

- If you have specified a file-level restore from a storage system backup, if you enabled warning messages, and if file overwrite or out-of-space conditions exist, the **Restore** wizard displays warning messages that list the files for which those conditions apply.
- In all other cases, the **Restore** wizard displays no warnings.

9. If the **Restore** wizard displays no file overwrite or out-of-space warnings that require correction, click **Next**.

The **Restore** wizard displays the volumes, qtrees, directories, or backup files that will be restored and the location in which they will be restored.

10. If the **Restore** wizard displays file overwrite or out-of-space warnings, that require correction, cancel the **Restore** wizard operation, correct the conditions, and restart the **Restore** wizard again.

11. (Optional) To receive desktop notifications of your job status, click **Notify on job progress**.

A job alert dialog box will appear in the lower right-hand corner of your screen.

12. Click **Finish** to end the wizard start the restore operation.

#### After you finish

- You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.
- After the licensed protection application restores the data, to protect the data, you must add it to a dataset.

#### Related references

[Administrator roles and capabilities](#) on page 1055

# Restoring backed-up data over current data

---

You can overwrite current data with their restored copies. You can restore backed-up data over existing data if you suspect that the current files in a dataset are corrupted.

## Before you begin

- Before restoring backed-up data over current data, ensure that the following conditions are true:
    - You know the backup version that you want to restore.
    - You know which volumes, qtrees, directories, files or Open System SnapVault directories you want to restore.
    - If you are restoring a LUN, and your protection application is not configured to support non-disruptive LUN restore, the LUN in the destination location is offline.
    - If your protection application is configured to support non-disruptive LUN restore and you are restoring to a LUN that is owned by a vFiler unit, that vFiler unit is a primary vFiler unit.
- Note:** Performing non-disruptive restore to a LUN owned by a vFiler unit restores the backed-up LUN without its original LUN mappings and the restored LUN must be remapped.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
  2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that includes the files that you want to restore.
  3. Click **Restore** to start the **Restore** wizard.
- The wizard displays the **Backup Files** window.
4. If you want the **Restore** wizard to warn of file overwrite or out-of-space conditions during a file-level restore, select **Warn about overwrite and out-of-space conditions on the destination**.

**Note:** This option enables warnings only for file-level restores from storage system backups. The **Restore** wizard does not issue file overwrite or out-of-space warnings for volume-level restores, qtree-level restores, folder-level restores, restores from Open Systems SnapVault backups, or restores from ESX server backups.

5. From the list of backups in the left pane, select the backup copy that you want to restore.

All backup copies are displayed by their backup dates and their dataset descriptions. All backup files that belong to the restored data are displayed in the right pane. Currently unavailable copies are marked as such.

6. Select the volumes, qtrees, directories and files contained in the backup copies that you want to restore and click **Next**.

You can select multiple volumes, qtrees,directories, or files simultaneously.

7. In the **Restore Preferences** window, click **Original location** to overwrite current data with the restored data and click **Next**.

8. The **Restore** wizard executes a dry run of your request and tests for warning conditions.

- If you specified a file-level restore from a storage system backup, enabled file overwrite or out-of-space warnings, and file overwrite or out-of-space conditions exist, the **Restore** wizard displays warning messages that list the files for which those conditions apply.
- In all other cases, the **Restore** wizard displays no warnings.

9. If the **Restore** wizard displays no file overwrite or out-of-space warnings that require correction, click **Next**.

The **Restore** wizard displays the volumes, qtrees, directories, or backup files that will be restored and the location in which they will be restored.

10. If the **Restore** wizard displays file overwrite or out-of-space warnings, that require correction, cancel the **Restore** wizard operation, correct the conditions, and restart the **Restore** wizard again.

11. (Optional) To receive desktop notifications of your job status, click **Notify on job progress**.

A job alert dialog box will appear in the lower right-hand corner of your screen.

12. Click **Finish** to end the wizard start the restore operation.

### After you finish

- You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.
- If you performed a non-disruptive LUN restore to LUNs owned by a vFiler unit, you must restore the LUN mappings that were lost during the restore.

### Related references

[Administrator roles and capabilities](#) on page 1055

# Restoring selected portions of a dataset

---

You can start the **Restore** wizard and initiate restoring portions of a dataset.

## Before you begin

- Before restoring portions of a dataset, ensure that the following conditions are true:
  - You know the backup version that you want to restore. All backup copies are displayed by their backup dates and dataset descriptions.
  - You know which files and directories you want to restore.
  - You know the location to which you want to restore backups.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

- 

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that you want to restore.
3. Click **Restore** to start the **Restore** wizard.
4. Complete the steps in the **Restore** wizard.

## After you finish

- You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.
- To receive e-mail notifications of your job status, click **Notify on job progress** on the Completing the Restore Wizard screen of the **Restore** wizard

## Related references

[Administrator roles and capabilities](#) on page 1055



# Restoring a virtual machine to its original location

You can restore a virtual machine to its original location. When the restore completes, Open Systems SnapVault returns power to the virtual machine.

## Before you begin

- Before restoring a virtual machine to its original location, ensure that the following conditions are true:
  - You know the backup version that you want to restore.
  - You know if you want to restore the entire virtual machine including its configuration, or just the data.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that includes the virtual machines that you want to restore.
3. Click **Restore** to start the **Restore** wizard.
4. In the **Backup Files** window, from the list of backups on the left, select the backup copy that you want to restore.

All backup copies are displayed by their backup dates and their dataset descriptions. Currently unavailable copies are marked as such.

**Note:** Do not enable the "Warn about overwrite and out-of-space conditions on the destination" option. The **Restore** wizard does not issue file overwrite or out-of-space warnings for restores from Open Systems SnapVault backups.

5. From the list of backup files on the right, select the type of information you want to restore and click **Next**.  
If you select Data, the restored information includes the data (VMDK) files. If you select Configuration, the restored information also includes the configuration files, including .vxm, .vmsd, .vmxf, .nvr, and vmware.log. You cannot restore the configuration files without also restoring the data files.
6. In the **Restore Preferences** window, click **Original location** to overwrite current data with the restored data and click **Next**.

The **Restore** wizard displays the backup files to be restored.

7. Click **Finish** to end the wizard and start the restore operation.

After the restore operation is complete, Open Systems SnapVault restarts the virtual machines.

#### **After you finish**

You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Restoring a virtual machine file system to any location

---

You can restore a backed-up virtual machine as files to any location. You can restore virtual machine file systems to a new location if the original data store that hosted the virtual machine does not exist anymore or if you want to test the file system when it is not installed on a server. At the completion of the restore, you will need to use VMware tools to configure and power on the virtual machine.

## Before you begin

- Before restoring virtual machine file systems to a new location, ensure that the following conditions are true:
  - You know the backup version that you want to restore.
  - You know if you want to restore the entire virtual machine which includes the configuration, or just the data.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that includes the VM files that you want to restore.
3. Click **Restore** to start the **Restore** wizard.
4. In the **Backup Files** window, from the list of backups on the left, select the backup copy that you want to restore.

All backup copies are displayed by their backup dates and their dataset descriptions. Currently unavailable copies are marked as such. All backup files that belong to the restored data are displayed on the right.

**Note:** Do not enable the "Warn about overwrite and out-of-space conditions on the destination" option. The **Restore** wizard issues file overwrite or out-of-space warnings only for file-level restores from storage system backups.

5. From the list of backup files on the right, select the type of information you want to restore and click **Next**.

If you select Data, the restore process includes the data (VMDK) files. If you select Configuration, the restore process also includes the configuration (vmx) files. You cannot restore the configuration files without also restoring the data files.

6. In the Restore Preferences window, select **Choose a location** to save the virtual machine as files to a new location and click **Next**.
  7. In the Restore Path window, either select the directory path in which you want to restore the files or type the directory path in the Restore path field, then click **Next**.
- The **Restore** wizard displays the backup files to be restored and the location in which the files are restored.
8. Click **Finish** to end the wizard and start the restore operation.

At the completion of the restore operation, you will need to use VMware tools to configure and power on the virtual machine.

#### **After you finish**

You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Restoring a virtual machine to its original location through another ESX server

---

You can restore a virtual machine to its original location through another ESX server as long as the new ESX server has access to the same data stores as the original ESX server.

## Before you begin

Before restoring backed up data to its original location through a different ESX server, ensure that the following conditions are true:

- Before restoring a virtual machine to its original location, ensure that the following conditions are true:
  - You know the backup version that you want to restore.
  - You know if you want to restore the entire virtual machine including its configuration, or just the data.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can restore a virtual machine using another ESX server if the original Open Systems SnapVault host that backed up the virtual machine does not exist anymore. You can also restore a virtual machine using another ESX server if the original ESX server is heavily loaded and you want to distribute the workload. If the original ESX server is not online when the virtual machine is restored, you will need to register the virtual machine to the new ESX server and power on the virtual machine using VMware tools.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. From the list of datasets in the Overview tab of the **Datasets** window, select the dataset that includes the backup files that you want to restore.
3. Click **Restore** to start the **Restore** wizard.
4. In the **Backup Files** window, from the list of backups on the left, select the backup copies that you want to restore.

All copies are displayed by their backup dates and their dataset descriptions. Currently unavailable copies are marked as such.

**Note:** Do not enable the "Warn about overwrite and out-of-space conditions on the destination" option. The **Restore** wizard does not issue file overwrite or out-of-space warnings for restores from Open Systems SnapVault backups.

- From the list of backup files on the right, select the type of information you want to restore and click **Next**.

If you select Data, the restored information includes the data (VMDK) files. If you select Configuration, the restored includes the configuration (vmx) files. You cannot restore the configuration files without also restoring the data files.

- In the **Restore Preferences** window, click **Choose an ESX Server** to restore the files to a new ESX server and click **Next**. (The list shows only ESX hosts that can be used for restoring.)
- In the **ESX Server** window, choose the ESX server to which you want to restore the virtual machines and click **Next**.

Only ESX servers that have access to all the data stores used by all the virtual machines you want to restore are available for selection.

The **Restore** wizard displays the backup files to be restored and the location to which the virtual machines are restored.

- Click **Finish** to end the wizard and start the restore operation.

Restoring a virtual machine to a new ESX server does not assign that virtual machine to that ESX server. You must reassign the virtual machine through VMware's VirtualCenter.

### After you finish

- You can use the **Jobs** window to track the progress of the restore job and monitor the job for possible errors.
- After the licensed protection application restores the data, to protect the data, you must add it to a dataset.

### Related references

[Administrator roles and capabilities](#) on page 1055

## About unprotected data

---

Data that does not belong to a dataset is not protected by the licensed protection application, even if that data is backed up by SnapVault or mirrored by SnapMirror software. To protect this data, you can import these external SnapVault and SnapMirror relationships into a dataset to which a protection policy is assigned. After the relationships are imported, the data is protected by the licensed protection application as defined in the protection policy.

When you first set up the licensed protection application, or add storage or vFiler units to systems using the licensed protection application, the data and protection relationships from the imported systems are displayed on the Resources tab, Datasets tab, and External Relationships tab that are accessed from the **Unprotected Data** window.



# Where to view unprotected data

---

The three tabs on the **Unprotected Data** window provide information about resources and external relationships that are not in a dataset and about datasets that are not yet associated with a protection policy.

**Datasets tab** The **Unprotected Data** window Datasets tab shows datasets that do not have protection policies assigned to them.

From this tab, you can do the following actions:

- View the Name, Description, Owner, and Contact properties for each unprotected dataset.
- Select an unprotected dataset and assign a protection policy and destination resources to that dataset.

**Resources tab** The **Unprotected Data** window Resources tab allows you to view storage system hosts, aggregates, volumes, or qtrees containing data that is not assigned to a dataset and is, therefore, not protected.

**Hosts button** You can perform the following actions by clicking this button:

- Assign the unprotected data to an existing dataset or create a new dataset to contain the data.
- View the Ignore status of a host and view the property details of hosts.
- Filter the display to ignore data that you do not want to protect by setting the Ignored flag to Yes on that data.

When you set the Ignore option to Yes for a host, the host name is removed from the host list. However, the host and its contents remain available to the licensed protection application. You can assign the Ignore property only to a host. You cannot ignore specific volumes or aggregates. By default, the hosts displayed in the **Unprotected Data** window are those that are not ignored, but you can filter the list by using the button to select All (all hosts, both ignored and not ignored), Yes (only hosts that are ignored), or No (only hosts that are not ignored).

Examples of when you might ignore a host include the following:

- You have a host that contains unprotected data, and you do not intend to protect that data.
- You have Open Systems SnapVault directories that you do not want to back up.

- You plan to protect data later and you want to keep the host data from being accidentally assigned to a dataset when it should not be.

**Aggregates button** You can assign the unprotected data to an existing dataset or create a new dataset to contain the data.

**Volumes button** You can assign the unprotected data to an existing dataset or create a new dataset to contain the data.

**Qtrees button** You can assign the unprotected data to an existing dataset or create a new dataset to contain the data.

**External Relationships tab** The **Unprotected Data** window External Relationships tab lists all unprotected SnapVault and SnapMirror (volume and qtree) relationships.

These relationships are listed here because they are not managed by the Protection Manager or Provisioning Manager applications.

From this tab, you can perform the following actions:

- View the Source, Type, Destination, and Lag properties for external relationships that were not imported into a dataset.
- Select one or more discovered relationships to import into a dataset.  
After importing to the dataset, the licensed protection application adds the source qtrees, volumes, directories, and the destination volumes and qtrees, to the destination node.

You can sort each column in these tabs by clicking the column header. The small arrow in the header indicates whether the entries are sorted in ascending or descending order. To reverse the sort order, click the column header again.

Each column header also contains a text field or a drop-down filter list, accessible by clicking the  icon. This filter option enables you to reduce the number of items listed. You can filter the entries in the columns by entering a term in the text field or by selecting an item from the filter list.

You can also filter the list content by using the Group selector on the console tool bar. When you select a group filter, only relationships originating or terminating at an object in the selected group are listed.

# Hosts that contain unprotected data

---

You can view and manage the data in host resources that are not yet protected, that is, data not yet in a dataset, by using the Hosts tab on the **Unprotected Data** window.

## Related concepts

[\*How hosts become visible to the console\*](#) on page 901



## When to import discovered relationships

---

You should use the External Relationships tab of the **Unprotected Data** window to import a discovered relationship when you have identified that the relationship is not managed by the licensed protection application.

After you import discovered relationships, the licensed protection application takes over the management of data protection schedules and policies, and it disables the schedules and policies that were previously managed by Backup Manager.

If you import a Volume SnapMirror relationship into Protection Manager, the original mirror schedule is preserved. Protection Manager monitors the relationship, but does not execute the schedule.

You should also import discovered relationships in the following situations:

- You installed Protection Manager and are setting up data protection for the first time.
- You added storage resources to resource pools.
- You added unprotected or unmanaged relationships to the licensed protection application.
- You added existing SnapVault or SnapMirror relationships to datasets.

There are two ways of handling existing SnapVault relationships:

- The DataFabric Manager server discovers the SnapVault relationship and does not manage it. The storage systems involved in the protection relationship control the protection schedule and retention policy.
- The DataFabric Manager server discovers the relationship, and you decide to manage the protection schedule and retention policy from the Operations Manager Web-based user interface. In this situation, you create the protection schedule and policy using Operations Manager and assign them to the relationship.



# **Adding unprotected host data to an existing dataset**

You can add unprotected data to an existing host dataset, even if the dataset is currently unprotected. You can browse or add data from an entire host, or from individual aggregates, volumes, qtrees, Open Systems SnapVault directories, or virtual machines on the host.

## **Before you begin**

- Determine the name of the dataset to which you want to add the unprotected data.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## **About this task**

When you add an unprotected qtree or volume to a dataset that has an assigned protection policy, the protection application initiates an initial baseline transfer of the qtree's or volume's data from the primary to the secondary node of the dataset. An initial baseline transfer of existing qtree or volume data might require many times more bandwidth and time than subsequent incremental transfers of that data will require.

## **Steps**

1. From the navigation pane, click **Data > Unprotected Data > Resources**.

2. Select the data that you want to add to a dataset:

- a. Select the name of the host that contains the data that you want to protect.

The aggregates, volumes, qtrees, and virtual machines contained in that host are displayed in the bottom left pane, in a hierarchical list.

- b. (Optional) Select the aggregates, volumes, trees, files, virtual machines, or Open Systems SnapVault directories that contain the data that you want to protect.

You can select multiple items from either list by using Ctrl-Click or Shift-Click. You can also select a host from the list to add all the data on the host to the dataset.

3. Click **Add to existing Dataset**.

A dialog box opens, from which you can select an existing dataset. This list includes both protected and unprotected datasets.

**Note:** If you add the unprotected data to an unprotected dataset, the data remains unprotected until you associate the dataset with a protection policy.

- You can verify that the existing dataset contains the new host data by viewing the dataset member list in the **Datasets** window Overview tab.

- You can determine whether the dataset to which you added the data is protected or unprotected. If the dataset name appears on the **Unprotected Data** window Datasets tab, then the dataset is not protected.
- If the dataset is unprotected and you want to protect the data in the dataset, you must associate the dataset with a protection policy. Go to the **Datasets** window Overview tab to complete the appropriate tasks.
- To create an on-demand backup copy of a protected dataset, go to the **Datasets** window, select the dataset, then click **Protect Now**.

#### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Adding unprotected host data to a new dataset

---

If there is no existing dataset that meets the requirements of your unprotected host data, you can create a new dataset for your data. You can browse or include data from an entire host, or from individual aggregates, volumes, qtrees, virtual machines, or directories on the host.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Unprotected Data > Resources**.

2. Select the data that you want to add to a new dataset.

a. Select the name of the host that contains the data that you want to protect.

The aggregates, volumes, trees, and virtual machines contained in that host are displayed in the bottom pane, in hierarchical form.

b. (Optional) Select the aggregates, volumes, trees, files, virtual machines, or Open Systems SnapVault directories that contain the data that you want to protect.

You can select multiple items from either list by using Ctrl-Click or Shift-Click. You can also select a host from the list to add all the data on the host to the dataset.

3. Click **Add to new Dataset** to start the **Add Dataset** wizard.

4. Complete the steps in the wizard to create a new dataset for the unprotected data.

The qtrees, volumes, aggregates, virtual machines, or hosts that you included in the dataset are displayed in the **Datasets** window and are no longer displayed in the hierarchy or host lists in the **Unprotected Data** window.

- If you want to protect the data in the dataset, you must assign a protection policy to the dataset. If you did not apply a protection policy and node resources when you created the new dataset, go to the **Datasets** window to complete the appropriate tasks.
- To create an on-demand backup copy of the dataset, go to the **Datasets** window, select your new dataset, and click **Protect Now**.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Protecting unprotected datasets

---

You do not have to assign a protection policy when you create a dataset, but a dataset without an assigned policy is not protected by the licensed protection application. When you are ready to initiate protection for a dataset, you assign a protection policy to it and assign resources to the dataset nodes.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Unprotected Data ▶ Datasets**.
2. Select the dataset that you want to protect.
3. Click **Protect**.

The **Datasets** window Overview tab is displayed and the unprotected dataset is selected.

4. Click **Protection Policy** to start the **Dataset Policy Change** wizard.
5. Complete the steps in the wizard to assign a policy to the dataset.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Decisions to make before importing external relationships

---

Before you use the **Import Relationships** wizard to import external protection relationships into a dataset, you need to decide which dataset, if any, meets the requirements of the relationships, whether you need to create a new dataset, and which connection to associate with each external relationship.

## Selecting the dataset

- Is there an existing dataset that meets the requirements of the external relationships you want to import?

Review the existing datasets listed on the **Datasets** window Overview tab to see if any are suitable for the external relationships. Consider the policy applied to the dataset and the protection schedule used by the policy. Are the protection requirements of the other dataset members the same as for the external relationships that you want to import?

**Note:** You cannot import an Open Systems SnapVault host or directory into a dataset when a local backup schedule is already defined on the primary node. You can import them only into datasets that have policies specifying either no protection or remote backups only.

- When selecting a relationship to associate with a policy connection, did you take into consideration that the licensed protection application adds the source and destination storage objects to the dataset?

For example, when importing a SnapVault relationship, you select the source qtree or directory to be added to the source node, and the licensed protection application adds the destination volume to the destination node. If the user adds a VolumeSnapMirror relationship, the source and destination volumes are added to the corresponding datasets.

- If no existing dataset meets the requirements of the external relationships that you want to import, create a new dataset.

## Determining which connection to associate with a relationship

- Does the dataset that you selected have more than one connection to which you can import an external relationship? For example, a dataset protected by the "Chain of two mirrors" policy has two mirror connections into which you might import a SnapMirror relationship.

Review the policy settings for each connection and node and the resources assigned to each node to help you decide which connection is the better match for the external relationship.

- To review the policy settings for each connection and node in the dataset, go to the **Protection Policies** window, select the policy applied to the dataset, and then click **Edit > Nodes and Connections**.

- To review the resources assigned to each destination node in the dataset, go to the **Datasets** window Overview tab, select the dataset, and then in the Graph area, click the node that you want to check.

#### **Related tasks**

*[Importing discovered external relationships](#)* on page 451

# Importing discovered external relationships

---

The licensed protection application discovers existing external SnapVault and SnapMirror relationships. If you choose to manage an existing relationship using the protection application, you must import it into an existing dataset.

## Before you begin

- Have the relationship information available that you need to complete this task:
  - An existing dataset that meets the requirements of the external relationships
  - The connection to which you will associate the relationship
- Ensure that you have determined the dataset to which you will import the external relationships and the connections in that dataset that you will associate with each external relationship.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data** ▶ **Unprotected Data** ▶ **External Relationships**.
2. Select one or more relationships from the list and click **Import** to start the **Import Relationships** wizard.
3. Complete the steps in the wizard to import the relationships into an existing dataset.

The protection application imports the selected SnapVault or SnapMirror relationships into the dataset. These relationships are now treated as though the protection application created them.

## Related concepts

[Decisions to make before importing external relationships](#) on page 449

## Related references

[Administrator roles and capabilities](#) on page 1055



# What groups are

---

A *group* is a collection of objects with common characteristics, such as location, project, or owning organization.

The groups you create in the licensed protection and provisioning applications are the same as the resource groups you create in Operations Manager. You can create single-type groups of objects, or you can create groups that include combinations of object types. You can create groups of objects such as datasets, resource pools, storage systems, hosts, vFiler units, aggregates, volumes, and qtrees. Objects can be members of more than one group.

Combining objects in groups allows you to filter data for the objects in the group. Grouping datasets and resource pools also enables you to see consolidated reports of information in Operations Manager. See the Operations Manager online help for detailed descriptions of the default views for datasets and resource pools and the custom catalogs you can use to create your own reports.

**Note:** If necessary, you can use Operations Manager to specify Storage Resource Management or chargeback settings or to create groups containing other types of objects (LUNs, SRM paths, and so on).

## Related concepts

[NetApp Management Console data filtering](#) on page 35

[Overview of resource pools](#) on page 819

[Dataset concepts](#) on page 693

## Related tasks

[Changing dataset node resource assignments](#) on page 739



## What the global group is

---

By default, a group called Global exists in the DataFabric Manager database. All objects in the database (datasets, resource pools, agents, aggregates, volumes, qtrees, Open Systems SnapVault hosts, and NetApp storage systems) belong to the Global group, whether they are discovered, like storage systems, or created, like resource pools.

If you create a new group, you assign objects to the new group from the Global group. If an object is reassigned from one group to another, the object is still a member of the Global group.

You cannot delete or rename the Global group. However, you can use Operations Manager to delete objects from the Global group and add previously deleted objects to the Global group. When you delete an object from the Global group, DataFabric Manager stops monitoring and reporting data for the object. Data collection and reporting is not resumed until the object is added back into the database (“undeleted”).



# Group properties

---

You can use the following information when you configure or edit a group's properties.

<b>Name</b>	Group names can contain any printable ASCII character except a forward slash character. The maximum name length is 64 characters. Group names cannot be the reserved names "all" or "global" or fully numeric. If a group has a parent group, the name of the group must be unique only among the subgroups of its parent.
<b>Owner</b>	The name of the person who should be copied on all e-mail or pager alerts for this group.
<b>E-mail</b>	The e-mail address of the group owner.
<b>Parent</b>	The name of the current parent group.
<b>Members</b>	The names of the objects the group contains.

## Related tasks

[Adding groups](#) on page 461

[Editing groups](#) on page 463



# Decisions to make before adding groups

---

Before you use the **Add Group** wizard to create a new group, you need to decide what storage objects to include in this group and which people you want to give access to these storage objects.

**Note:** This topic applies only to the licensed protection and provisioning applications. You cannot add groups with Performance Advisor.

## Group properties

- What is the name of the new group?

You cannot name a new group "all" or "global." The group name cannot contain more than 64 characters or include a forward slash. It must contain at least one non-numeric character.

- Who is the owner of the group?

Determine which individuals or groups you want to have access to the storage objects in this group.

- If an event within the group triggers an alarm, who should be contacted?

Determine what the email address is for each person or distribution list that should be contacted.

## Group membership

- What storage objects do you want accessed by the same person or group?

- How granular do you want to be in selecting storage elements for membership in your group?

You can add specific aggregates, volumes, qtrees, storage systems, Open Systems SnapVault hosts, and datasets to a group. If you add a storage element to a group, all the elements contained in that storage element can be accessed by the owner of this group.

**Note:** In order to assign any of the objects mentioned, you need view permission for those objects.

## Related tasks

[Adding groups](#) on page 461



# Adding groups

---

You can add a group directly under the Global group or create a subgroup to a parent group you already created.

## Before you begin

To add a group, you must have the license enabled for either the protection application or provisioning application. You cannot add groups with Performance Advisor.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. When you add a group, you can add an object to the group membership only if you have permission to view that object.

Have the information available that you need to complete this task:

- Name of the group
- Owner of the group
- E-mail address of the owner
- Members to add to the group

## Steps

1. From the navigation pane, click **Data > Groups**.
2. Click **Add** to start the **Add Group** wizard.

Complete the steps in the wizard to create the new group.

The new group appears in the Group Name list.

## Related concepts

[Decisions to make before adding groups](#) on page 459

## Related tasks

[How do I back up data?](#) on page 589

## Related references

[Group properties](#) on page 457

[Administrator roles and capabilities](#) on page 1055



# Editing groups

---

You can edit the name, membership, or contact information for a group. This topic applies only to the licensed protection and provisioning applications. You cannot edit groups with Performance Advisor.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. When modifying group membership, you can see only the objects you have permission to view.

## About this task

If you rename a group, you are also changing the names of its subgroups, if any. The full name of any subgroup includes the names of groups in its parentage, so changes to the names of parent groups affect their subgroups as well.

## Steps

1. From the navigation pane, click **Data ▶ Groups**.
2. In the **Groups** window, select the group you want to edit.

You might need to expand the Group Name list to select the group you want.

Current information about the selected group appears in the Details area.

3. Click **Edit**.
4. In the group's **Properties** sheet, modify the group as needed.
5. Click **Apply** to save your changes or **OK** to save your changes and exit the dialog box.

The modified information about the selected group appears in the "Group name" or "Details" areas.

## Related tasks

[Deleting groups](#) on page 465

## Related references

[Group properties](#) on page 457

[Administrator roles and capabilities](#) on page 1055



# Deleting groups

---

You can delete groups that you no longer find useful. Deleting a group removes only the group container from the DataFabric Manager database. The objects contained in the deleted group are not removed from the database.

## Before you begin

**Note:** This topic applies only to the licensed protection and provisioning applications. You cannot delete groups using Performance Advisor.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

When you delete a group, you also delete all its subgroups, if any. If you want to preserve the subgroups, you must move them to a different parent group before deleting the current parent group. You can move one subgroup at a time in the protection and provisioning applications, or you can use Operations Manager to move multiple subgroups simultaneously. See the Operations Manager online Help for instructions.

## Steps

1. From the navigation pane, click **Data > Groups**.
2. In the Group Name list, select one or more groups that you want to delete.
3. Move any subgroups you want to retain.

Use the edit properties dialog box to move one subgroup at a time, or use Operations Manager to move multiple groups.

4. Click **Delete** to remove the group.  
A confirmation dialog box appears, asking whether you want to delete the selected groups.
5. Click **OK**.

Each selected group (and any subgroups) is deleted from the DataFabric Manager database. The Group name list is refreshed and no longer displays the deleted groups.

## Related tasks

[Editing groups](#) on page 463

## Related references

[Administrator roles and capabilities](#) on page 1055



# Monitoring jobs

---

You can monitor for job status and other job details using the **Jobs** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Jobs**.

Only jobs for the selected resource group are displayed.

2. (Optional) Customize the **Jobs** window in any of the following ways:

- Select a resource group to see the jobs for that group.
- Select a job in the jobs list to see the details about that job.
- Use the View Jobs filter buttons to control the range of jobs you want displayed.
- Click  in a column header to control which job entries you want displayed.
- Click the sort arrows in a column header to change the sort order of the entries in that column.
- Click  in the upper-right corner of the list to select which columns are displayed.
- Drag the bottom of the jobs list area up or down to resize that area.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Canceling jobs

---

You might need to stop a job: for example, if a job is taking too long to complete, if a job is encountering too many errors, or if a job was started manually but is no longer needed.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Jobs**.  
Only jobs for the selected resource group are displayed.
2. From the list of jobs, select one or more jobs that are currently running.  
The status in the Progress column must be **Running**.
3. Click **Cancel**.
4. In the Cancel Jobs dialog box, click **Yes** to stop the selected job.

The Cancel Job Request Process Monitor window displays the progress of your cancel request and detailed information about any errors that occurred during the cancellation process.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Where to view reports and logs

---

In general, you use your NetApp Management Console application to monitor jobs, events, and alarms associated with that application, and you use Operations Manager to monitor logs.

- To view reports of jobs, events, or alarms associated with most NetApp Management Console applications, use the NetApp Management Console System window.
- To view jobs, events, or alarms associated with your NetApp Management Console disaster recovery feature, use the Operations Manager Reports menu.

**Note:** After displaying the disaster recovery report, you can use the spreadsheet or print buttons to export the report to .XLS format or send it to the printer.

- To view DataFabric Manager or Operations Manager logs, use Operations Manager Reports menu.

**Note:** After displaying the report, you can use the spreadsheet or print buttons to export the report to .XLS format or send it to the printer.
- To view syslog cluster messages, use the tools available on the Operations Manager Cluster Console.

## Related tasks

[How do I back up data?](#) on page 589



# Dashboards > Protection

---

The protection dashboards provide cumulative at-a-glance status information for datasets, resource pools, protected data, and unprotected data. Further detail can be viewed on the Help page accessible from each dashboard panel.

The following dashboard panels can be viewed by administrators who have been assigned the appropriate privileges:

<b>Failover Readiness</b>	This panel is visible only if the disaster recovery feature is licensed on your system.  Indicates the status of datasets regarding their availability for failover, should failover action be required.
<b>Failover Status</b>	This panel is visible only if the disaster recovery feature is licensed on your system and if a dataset has failed over.  Provides feedback on active or completed failover operations.
<b>Top Five Events</b>	Displays the five most severe events from the <b>Monitor &gt; Events</b> list, ordered by time.
<b>Dataset Protection Status</b>	Displays the status of dataset protection policies and the number of datasets to which each status applies.
<b>Protected Data</b>	Displays the total number of each resource type covered by a protection policy, listed by the type of resource.
<b>Unprotected Data</b>	Displays the total number of each resource type not covered by a protection policy, listed by the type of resource.
<b>Dataset Lags</b>	Displays datasets that have a protection component that is out of date with respect to the primary data. This panel groups relationships according to their dataset, sorts relationships according to each relationship's lag, selects the longest lag for each dataset, and displays the datasets in decreasing order of lag.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to each resource pool and the amount of that total space that is being utilized. The Total Size is indicated in gigabytes or terabytes, and the Utilization is given in percentages of the total allocated space per resource pool. Items are sorted in decreasing order of available space.

Click  on the title bar of each dashboard panel to replace the work area with another window that is related to the content of the panel.

Click → on a row of a dashboard panel to replace the work area with a window that is related to the content of the panel, with information highlighted that is relevant to that specific row in the panel.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.

# Dashboards > Protection > Failover Readiness

You can use the **Failover Readiness** panel to view the readiness of datasets configured for disaster recovery protection to successfully carry out failover operations should failover operations become necessary. The panel lists the number of datasets whose failover support configurations are in ready state, warning state, and error state.

## Status Descriptions

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

<b>Failover Readiness</b>	The <b>Failover Readiness</b> panel only appears when the disaster recovery option is licensed. <ul style="list-style-type: none"><li>• Status: Normal Indicates that conditions in all datasets that are configured for disaster recovery protection will support successful failover operations if such operations become necessary. Nothing has changed in the configuration since the dataset was configured for disaster recovery.</li><li>• Status: Warning Indicates that conditions have changed in one or more datasets that are configured for disaster recovery protection so that failover operations might not be completely successful, if such operations become necessary. The datasets producing the warnings should be investigated and brought back into the Normal state.</li><li>• Status: Error Indicates that conditions have significantly changed in one or more datasets that have been configured for disaster recovery protection so that it is likely that failover operations will not be completely successful, if such operations become necessary, and data could be lost. The datasets producing the warnings should be investigated and brought back into the Normal state.</li></ul>
<b>Ready</b>	Total number of datasets that have been configured for disaster recovery protection whose conditions will support successful failover operations, if such operations become necessary.
<b>Ready - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection whose conditions might not support completely successful failover operations, if such operations become necessary.
<b>Error - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection to which significant changes have occurred to the configurations. Failover operations

can still occur but might not be completely successful, if such operations become necessary.

**Total Datasets** The total datasets that have been configured for disaster recovery protection.

Click  beside the dashboard panel title to replace the work area with the Disaster Recovery tab on the **Datasets** window.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.

# Dashboards > Protection > Failover Status

You can use the **Failover Status** panel to view the status of an in-progress failover operation. The panel appears when a failover operation is invoked, listing the number of datasets in the process of failing over and the number of datasets that have successfully failed over.

## Status Descriptions

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

<b>Failover Status</b>	The <b>Failover Status</b> panel only appears when the disaster recovery option is licensed. <ul style="list-style-type: none"><li>• Status: Normal. Indicates that failover operations are either successfully completed or are proceeding as expected in all datasets that have been configured for disaster recovery protection.</li><li>• Status: Warning Indicates that failover operations have completed with a warning condition in one or more of the datasets that have been configured for disaster recovery protection.</li><li>• Status: Error Indicates that failover operations have completed with an error condition in one or more of the datasets that have been configured for disaster recovery protection.</li></ul>
<b>Failing over</b>	Total number of datasets that have been configured for disaster recovery protection that are currently undergoing failover operations.
<b>Failed over</b>	Total number of datasets that have been configured for disaster recovery protection that have successfully completed failover operations.
<b>Failed over - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection that have completed failover operations with warning conditions. Warnings can be encountered during the failover operation or warnings that exists in the ready state, as shown in the Failover Readiness panel, can be propagated to the Failed Over state.
<b>Failed over - Errors</b>	Total number of datasets that have been configured for disaster recovery protection that have completed failover operations with error conditions. Errors can be encountered during the failover operation or errors that exists in the ready state, as shown in the Failover Readiness panel, can be propagated to the Failed Over state.

**Total Datasets** The total datasets that are issuing failover status events.

Click  beside the dashboard panel title to replace the work area with the Disaster Recovery tab on the **Datasets** window.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.

# Dashboards > Protection > Dataset Protection Status

---

You can use the **Dataset Protection Status** panel to view the overall status of each dataset protection policy. The panel lists the number of datasets to which each protection status value currently applies.

## Status Descriptions

The dashboard panel lists the status entries from least to most severe.

<b>Protected</b>	Status: Normal  Total number of datasets being protected according to their assigned policies
<b>Uninitialized</b>	Status: Normal  Total number of datasets for which there are no backups of the data
<b>Protection Suspended</b>	Status: Normal, paused  Total number of datasets for which an administrator has requested that scheduled backups be put on hold until the administrator requests that they be resumed
<b>Job Failure</b>	Status: Warning (the status is displayed in amber)  Total number of datasets for which an error occurred while protecting the data
<b>Lag Warning</b>	Status: Warning (the status is displayed in amber)  Total number of datasets nearing the lag threshold
<b>Lag Error</b>	Status: Error (the status is displayed in red)  Total number of datasets for which the protection lag has exceeded the configured threshold

Click  beside the dashboard panel title to replace the work area with the **Datasets** window.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.



## Dashboards > Protection > Protected Data

---

You can use the **Protected Data** panel to view the data resources that are covered by protection policies. Items are listed by the type of data resource.

The data types displayed in this dashboard panel include the following:

- Datasets
- Volumes
- Qtrees
- OSSV Directories (Open Systems SnapVault directories)

The data types in the list are mutually exclusive because some items might not be in datasets. If data is not yet protected by a policy, that data resource is not included in the totals provided in this dashboard panel.

Click  beside the dashboard panel title to replace the work area with the **Datasets** window.

You can filter the content of the dashboard panels to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.



## Dashboards > Protection > Unprotected Data

---

You can use the **Unprotected Data** panel to view the total number of data resources, listed by resource type, that are not covered by protection policies.

The data types displayed in the **Unprotected Data** panel include the following:

- Datasets
- Volumes
- Qtrees

The data types in the list are mutually exclusive because some items may not be in datasets.

If you set the Ignore property to Yes for an unprotected resource, that ignored resource is not included in the total numbers displayed on this dashboard panel.

Click  beside the dashboard panel title to replace the work area with the **Unprotected Data** window.

Click  beside Datasets to replace the work area with the **Unprotected Data** windowDatasets tab.

Click  beside Volumes to replace the work area with the **Unprotected Data** windowResources tab.

Click  beside Qtrees to replace the work area with the **Unprotected Data** windowResources tab.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selector on the console tool bar.



## Dashboards > Protection > Dataset Lags

---

You can use the **Dataset Lags** panel to identify datasets that have a protection component that is out of date with respect to the primary data. The panel displays relationships grouped according to their dataset, sorts relationships according to each relationship's lag, selects the longest lag for each dataset, and displays the datasets in decreasing order of lag time.

Click  beside the dashboard panel title to replace the work area with the **Datasets** window. You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.



## Dashboards ► Top Five Events

---

You can use the **Top Five Events** panel to view the five most severe events listed in the **Events** window and the source to which each event applies. The columns are ordered first by severity, then by time of the events.

Click  beside the dashboard panel title to replace the work area with the **Events** window. Descriptions of the events are provided in the online Help page for that window.

Click  on a row of the **Top Five Events** panel to replace the work area with the **Events** window, with information highlighted that is relevant to the selected row in the dashboard panel.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



# Data ▶ Datasets ▶ Overview

---

The **Datasets** window Overview tab provides a single location from which you can monitor the status of all datasets, create and modify datasets, and assign physical resources manually or by using provisioning policies. If you have the protection license, you can back up a dataset's content on demand, suspend or resume protection for it, and initiate restore operations to access backed-up data from this page.

- [Command buttons](#) on page 1033
- [Datasets list](#) on page 1034
- [Graph area](#) on page 1036
- [Details area](#) on page 1037
- [Window customization](#) on page 1039

## Command buttons

<b>Add</b>	Starts the <b>Add Dataset</b> wizard for adding a dataset.
<b>Edit</b>	Opens the <b>Edit Dataset</b> window, from which you can modify general properties of a dataset, physical resources of a dataset, or how storage is provisioned on a dataset.
<b>Delete</b>	Deletes the selected dataset and thereby removes the relationships among the storage resources.
<b>Protection Policy</b>	Starts the <b>Dataset Policy Change</b> wizard, from which you can select a protection policy and destination storage to associate with your dataset.
<b>Protect Now</b>	Opens the Protect Now dialog box, from which you can perform on-demand backup or mirror protection operations on datasets that are protection policy-enabled for those types of operations. This button is disabled for datasets that do not have a protection policy assigned.  If you click the box "Notify me on job progress," you receive desktop alerts about this job's status after starting the Protect Now process.
<b>Note:</b> With application datasets, clicking <b>Protect Now</b> copies all new backups that have not been copied to the secondary backup node. Protect Now does not create new local backups on the primary nodes of application datasets.	
<b>Suspend</b>	Suspends dataset protection or provisioning for one or more datasets.  During the time that the application suspends protection, it displays a Protection Suspended status for the dataset.  This button is enabled only if a protection or provisioning policy is assigned to the dataset.

**Note:** When you click the Suspend button to stop the protection for an application dataset, a note displays, reminding you that local backups that are being created by another application cannot be suspended.

**Resume** Resumes dataset backup protection or provisioning for one or more datasets.

**Restore** Starts the **Restore** wizard for restoring backed-up copies of data.

## Datasets list

Lists information about existing datasets.

**Name** The name of the dataset.

**Overall Status** The status determined by evaluating the combined status conditions for disaster recovery, protection, conformance, space, and resources.

Licensing is checked before determining whether any status contributes to the overall status. If a feature is not licensed, it is not considered when determining the Overall Status value.

The following table shows how overall status is computed based upon other status values.

Overall Status	DR status condition	Protection status condition	Conformance status condition	Space status condition	Resource status condition
Error	Error	Lag error Baseline failed	Nonconformant	Error	Emergency Critical Error
Warning	Warning	Job failure Lag warning Uninitialized No protection policy for a non-empty dataset		Warning	Warning
Normal					

<b>Protection Policy</b>	The name of the protection policy currently assigned to the dataset.
<b>Primary Provisioning Policy</b>	The name of the provisioning policy currently assigned to the primary node of the dataset. If a provisioning policy is assigned to a secondary node in the dataset, that name is displayed in the details area when you select the secondary node in the graph area.
<b>Failed Over</b>	Indicates whether a disaster recovery-capable dataset has failed over. Valid values are the following:
<b>Yes</b>	Failover on the dataset was invoked and completed successfully, completed with warnings, or completed with errors.
<b>No</b>	Failover on the dataset has not been invoked.
<b>In Progress</b>	Failover on the dataset is currently in progress.
<b>Not Applicable</b>	The dataset is not assigned a disaster recovery protection policy and, therefore, is not capable of failover.
<b>Description</b>	A description of the dataset.
<b>Protection Status</b>	Displays protection status. This column is not shown by default and is not available if the protection application is not licensed.  Valid values, in alphabetical order, are as follows:
<b>Baseline Failed</b>	The dataset's initial baseline transfer did not succeed. Check the conformance status for more information.
<b>Initializing</b>	The dataset is in conforming state (becoming conformant) and its initial baseline transfer is taking place.
<b>Job Failure</b>	The most recent protection operation for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded the lag error threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.

<b>Lag Warning</b>	The dataset has reached or exceeded the lag warning threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>No Protection Policy</b>	The dataset is managed by the protection application, but no protection policy has been assigned to the dataset.
<b>Protected</b>	The data is being protected according to policy.
<b>Protection Suspended</b>	Protection for the dataset has been suspended.
<b>Uninitialized</b>	The dataset does not have any data in it, or it has only one node and its assigned policy has no schedule configured, or it has only one node and the backup Snapshot copy schedule for the assigned policy has not started any jobs.
<b>Space Status</b>	If you have the Provisioning license, displays the status of the available space for the selected dataset node (OK, Warning, Error, or Unknown). If any member of a dataset has space allocation error or warning conditions, the dataset's space status indicates that condition. You can select the dataset to scan its volumes, LUNs, or qtrees to determine which member is the cause of the warning or error condition. This item is not included in the dataset list by default.
<b>Conformance Status</b>	For the licensed protection application, indicates whether the dataset is Conformant, Nonconformant, or In Progress.
<b>Resource Status</b>	The most severe of all current events on all direct and indirect members of the dataset nodes. Values can be Emergency, Critical, Error, Warning, or Normal. This item is not included in the dataset list by default.
<b>Application</b>	The name of the application that created the application dataset, such as SnapManager for Oracle. This item is not included in the dataset list by default.
<b>Application Version</b>	The version of the application that created the application dataset. This item is not included in the dataset list by default.
<b>Application Server</b>	The name of the server that runs the application that created the application dataset. This item is not included in the dataset list by default.

## Graph area

The graphical representation of the nodes for the selected dataset are displayed in the lower section of the page. Click the node or connection on which you want to view status and configuration details.

## Details area

The details of the selected dataset node are displayed next to the graph area. Click  to view member details, status details, or resource details about the selected primary, secondary, or tertiary node.

<b>Primary data or Disaster recovery data node details</b>	If you select the Primary data node or the DR data node in the Graph area, the details area displays the following status and configuration information about the selected node.
<b>Protection</b>	Displays protection status. This item is not shown if the protection application is not licensed.  Valid values are as follows:
<b>Protected</b>	The data is being protected according to policy.
<b>No Protection Policy</b>	No protection policy is assigned to the dataset.
<b>Job Failure</b>	Protection for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded a lag threshold.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>Lag Warning</b>	The dataset is approaching a lag threshold.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>Protection Suspended</b>	Protection for the dataset has been suspended.
<b>Uninitialized</b>	There are no backups for the dataset.
<b>Conformance</b>	For the licensed protection application, indicates whether the dataset is conformant. If a dataset is nonconformant, click  to evaluate errors and warnings and to run the conformance checker.

<b>Resource</b>	For the licensed protection application, represents the most severe of all current events on all direct and indirect members of the dataset nodes. Values can be Emergency, Critical, Error, Warning, or Normal. For Emergency, Critical, Error, or Warning conditions, click  to evaluate the events and sources causing those conditions.								
<b>Space</b>	For the licensed provisioning application, displays the status of the available space for the selected dataset node (OK, Warning, Error, or Unknown). If any volume, qtree, or LUN of a dataset has space allocation error or warning conditions, the dataset's space status indicates that condition. You can select the dataset to scan its volumes, LUNs, or qtrees to determine which member is the cause of the warning or error condition.								
<b>Failover</b>	Uses color, icons, and text to display the state and status of a dataset that is capable of disaster recovery. The colors and text vary according to the status of the activity. The state of a dataset can be Ready, Failing Over, or Failed Over. The status of an activity can be Normal, Warning, or Error.								
<b>Physical resources</b>	Displays the physical resources assigned to the selected dataset node. Click  for details.								
<b>Resource pools</b>	Displays the name of the resource pool. Click  for details.								
<b>Exports</b>	Displays information about the export settings applied to the selected dataset.								
<b>Local backup schedule</b>	Displays the name of the local backup schedule assigned to the protection policy of the selected dataset node.								
<b>Backup versions</b>	Lists local backups for a given dataset to help you select the files or directories to restore, or, if a volume has more backup versions than specified by its retention settings, which backup versions to delete.								
<b>Dataset properties details</b>	Depending on the properties of the selected dataset, the licensed protection application displays some or all of the following details. <table><tr><td><b>Owner</b></td><td>Owner of the current dataset.</td></tr><tr><td><b>Contact</b></td><td>E-mail contact address for this dataset.</td></tr><tr><td><b>Time zone</b></td><td>Time zone in which the dataset is located.</td></tr><tr><td><b>Application</b></td><td>(Displayed for application datasets) The application that generated the dataset.</td></tr></table>	<b>Owner</b>	Owner of the current dataset.	<b>Contact</b>	E-mail contact address for this dataset.	<b>Time zone</b>	Time zone in which the dataset is located.	<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.
<b>Owner</b>	Owner of the current dataset.								
<b>Contact</b>	E-mail contact address for this dataset.								
<b>Time zone</b>	Time zone in which the dataset is located.								
<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.								

<b>Application version</b>	(Displayed for application datasets) The application version that generated the dataset.
<b>Application server</b>	(Displayed for application datasets) The name of the application server that generated the dataset.
<b>Connection details</b>	If you select a backup or mirror connection in the Graph area, the details area displays the following information about that connection:
<b>Relationships</b>	Displays the number of existing relationships for the selected connection. Click  for relationship details.
<b>Schedule</b>	Displays the name of the schedule that is assigned to the selected backup connection.
<b>Throttle</b>	Displays the name of the throttle schedule, if any, that is assigned to the selected connection.
<b>Lag status</b>	Displays the current lag status for the selected connection. If error or warning conditions exist, click  for details.
<b>Backup or Mirror node details</b>	If you select a Backup node or a Mirror node in the Graph area, the details area displays the following information about that node:
<b>Provisioning policy</b>	Lists the provisioning policies, if any, that are assigned to the selected node.
<b>Physical resources</b>	Lists the physical resources that are assigned to the selected node. Click  for details.
<b>Resource pools</b>	Lists the resource pools, if any, that are assigned to the selected node. Click  for details.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.

- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Datasets > Disaster Recovery

---

You can use the Disaster Recovery tab to perform monitoring, update, testing, and failover tasks on datasets if you have installed the Disaster Recovery license.

- [Command buttons](#) on page 659
- [Datasets list](#) on page 659
- [Graph tab](#) on page 660
- [Jobs tab](#) on page 662
- [Window customization](#) on page 663

## Command buttons

<b>Failover</b>	Starts the process for primary-to-disaster recovery node failover in the selected disaster recovery enabled dataset.
<b>Test</b>	Tests the validity of user-defined failover scripts specified in the disaster recovery protection policy that is assigned to the selected dataset.
<b>Update</b>	Starts an immediate primary-to-disaster recovery node update in the selected dataset.  This operation is most likely invoked in preparation for an impending event that can potentially disable a primary storage facility and necessitate failover to a disaster recovery-enabled backup site, but is still distant enough to allow completion of a final backup of data from a primary storage node to its disaster recovery-enabled node.
<b>Cancel</b>	Cancels any update or failover operation in the selected dataset.

## Datasets list

Displays a table of all datasets enabled for disaster recovery protection.

<b>Name</b>	The name of the dataset.
<b>Failover</b>	The failover status of the dataset. Possible statuses include the following:
<b>Ready</b>	The dataset is ready for failover.
<b>Failing over</b>	The dataset is in the process of failover.
<b>Failed over</b>	The dataset has completed successful failover.
<b>Failed over - Warning</b>	The dataset completed failover with warnings.
<b>Failed over - Error</b>	The dataset encountered errors during failover. Failover is not successful.

**Failover** The current status of the data backup between the primary data node and the disaster recovery node. Valid values, in alphabetical order, are as follows:

<b>Baseline Failed</b>	The dataset's initial baseline transfer did not succeed. Check the conformance status for more information.
<b>Initializing</b>	The dataset is in conforming state (becoming conformant) and its initial baseline transfer is taking place.
<b>Job Failure</b>	The most recent protection operation for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded the lag error threshold specified in the assigned protection policy.
<p><b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.</p>	
<b>Lag Warning</b>	The dataset has reached or exceeded the lag warning threshold specified in the assigned protection policy.
<p><b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.</p>	
<b>No Protection Policy</b>	The dataset is managed by the protection application, but no protection policy has been assigned to the dataset.
<b>Protected</b>	The data is being protected according to policy.
<b>Protection Suspended</b>	All protection operations between the primary node and disaster recovery node have been suspended.
<b>Uninitialized</b>	The dataset does not have any data in it, or it has only one node and its assigned policy has no schedule configured, or it has only one node and the backup Snapshot copy schedule for the assigned policy has not started any jobs.

**Description** A description of the dataset.

## Graph tab

Displays a selectable topological representation of the primary node, disaster recovery node, backup connections, and any other secondary node assigned to the selected dataset. Clicking a node or connection displays failover status and resource information about that node that you might need to evaluate prior to starting failover.

**Status**

<b>Primary Data node details</b>	If the primary storage node is selected, the licensed protection application displays the following primary storage node data:
<b>Protection</b>	The status of the data protection scheme assigned to this dataset (protected, uninitialized, suspended, lag warning, or lag error).
<b>Conformance</b>	Whether or not provisioning conformance errors exist in the selected node. If error conditions exist, click  for details.
<b>Resource</b>	Whether or not error or critical conditions exist in the resources assigned to the selected node.
<b>Space</b>	Whether or not space issues exist on the selected node. If warning or error conditions exist, click  for details.
<b>Failover</b>	The failover state of the primary data node.
<b>Physical resources</b>	Listing of the physical systems assigned to the selected node. Click  for details.
<b>Resource pools</b>	Resource pools, if any, that are assigned to provision the selected node.
<b>Local backup schedule</b>	The name of the local backup schedule, if any, that is assigned to the selected node. Click  for a graphical display of the exact backup times.
<b>Backup versions</b>	Listing of Snapshot copies stored on this node.
<b>Dataset properties details</b>	Depending on the properties of the selected dataset, the licensed protection application displays some or all of the following details.
<b>Owner</b>	Owner of the current dataset.
<b>Contact</b>	E-mail contact address for this dataset.
<b>Time zone</b>	Time zone in which the dataset is located.
<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.
<b>Application version</b>	(Displayed for application datasets) The application version that generated the dataset.
<b>Application server</b>	(Displayed for application datasets) The name of the application server that generated the dataset.

**Connection details** If the connection element is selected, Protection Manager displays the following data in connection with the data protection connections:

<b>Relationships</b>	The protection relationships between a source and target nodes.
<b>Schedules</b>	The name of the protection schedule assigned to this protection connection.
<b>Throttle</b>	The name of the throttle schedule assigned to this protection connection.
<b>Lag status</b>	The current lag status (good, warning, or error) of successfully completed protection backup or mirror operations between the source and target nodes. If error or warning conditions exist, click  for details.

**Backup Node** If the backup node is selected, Protection Manager displays the following data in connection with the data protection backup node:

<b>Node name</b>	The default or user-assigned name of the backup node.
<b>Provisioning policy</b>	The provisioning policy, if any, that is assigned to the backup node.
<b>Physical resources</b>	The physical resources assigned to the selected node. Click  for details.
<b>Resource pools</b>	The resource pools, if any assigned to the selected node. Click  for details.

## Jobs tab

Displays a log listing of the disaster recovery update and failover operations initiated on this dataset.

<b>Job</b>	A list of the jobs related to disaster recovery-related protection configuration or execution that the protection application has executed.
<b>Step</b>	A list of the phases or milestones that occurred or were attempted during the execution of the listed jobs.
<b>Time stamp</b>	The times and dates that the listed jobs and steps started or occurred.
<b>Result</b>	The Normal, Warning, or Error result status of the listed jobs or steps.

**Note:** You can select each listed job or step to display further details on that job or step in the pane to the right.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data > Datasets > Migration

---

You can use the Migration tab to start, complete, and clean up after a data migration. This tab is displayed only when the provisioning license is installed.

- [Command buttons](#) on page 503
- [Datasets list](#) on page 504
- [Details area](#) on page 505
- [Jobs tab](#) on page 507
- [Window customization](#) on page 508

## Command buttons

The migration command buttons are disabled when a dataset or vFiler unit migration is in progress.

<b>Start migration</b>	Initiates the first phase of a dataset migration by starting the <b>Dataset Migration</b> wizard, which begins a baseline transfer of the dataset. You must specify a destination storage system and an interface for each of the source vFiler unit's IP addresses. If VLANs need to be created, you must also specify the VLAN.
<b>Update</b>	Performs an on demand update of the SnapMirror relationships that were created as part of the "Start migration" operation. This button is enabled only when the "Start migration" operation has finished for the selected dataset.
<b>Cutover</b>	Initiates the second phase of a migration, which performs a cutover (in other words, switches the source from the old storage from which the data is served to the new storage destination). This button is enabled only when the migration start operation has finished for the selected dataset.
<b>Cancel</b>	Cancels the migration in progress for the selected dataset by stopping the migration process and returning the dataset to the status it had before the migration started. All ongoing data transfers for the migration are aborted, and the provisioned destination storage and destination vFiler unit are deleted. (You must manually delete VLANs and IPspaces that were created during the migration process.) This button is enabled during the migration start and update operations.
<b>Cleanup</b>	Initiates the third phase of a migration, which deletes the old storage from which the dataset was migrated. A preview window lists which volumes are to be destroyed as part of cleanup operation. VLANs and IPspaces used by the source vFiler unit are not automatically destroyed. This button is enabled only when a migration cutover process has finished for the selected dataset.
<b>Relinquish migration capability</b>	Deletes the vFiler unit that was created during provisioning, which makes the dataset no longer capable of being migrated.

## Datasets list

Displays a list of all the datasets in the selected group that are capable of data migration.

**Name** The name of the dataset.

**Migration status** The status of datasets capable of migration. The description, source storage status, destination storage status, permitted operations, and prohibited operations for each status are described as follows.

**Not started** The dataset meets the dataset migration requirements.

- Source storage system: Online
- Destination storage : Not provisioned
- Operations permitted: All
- Prohibited operations: Migration cutover, migration update, migrate complete, migration cancel, migration cleanup

You can initialize the start migration operation on datasets having a "Not started" or "Migrate failed" status.

**In progress** The baseline transfer of this dataset has started.

- Source storage system: Online
- Destination storage : Provisioned for the dataset then offline
- Operations permitted: Migration cancel
- Prohibited operations: Add or delete dataset volumes, provision storage for the dataset, edit provisioning or protection policies

**Started, cutover required** The migration start operation baseline transfer to the new destination storage system is finished. The dataset source needs to be switched to the new destination storage system.

- Source storage system: Online
- Destination storage : Online
- Operations permitted: Edit provisioning or protection policies, migration update, migration cutover, migration cancel
- Prohibited operations: Migration cleanup

**Migrated, cleanup required** The migration cutover operation is finished and the dataset is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. Old storage needs to be deleted.

- Source storage system: Offline
- Destination storage : Online

- Operations permitted: Resize storage, delete Snapshot copies, add and delete dataset volumes, provision storage for the dataset, edit provisioning or protection policies, migration cleanup
- Prohibited operations: Migration start, migration cancel, migration update, migration cutover

**Migrated with errors** The migration cutover operation successfully performed the switch to the destination storage system. However, a failure occurred during the migration of the backup version, backup relationships, or history for the primary data. You must manually correct the errors, change the migration status of the dataset using the Operations Manager CLI, and resume the dataset.

- Source storage system: Offline
- Destination storage : Online
- Operations permitted: Resize storage, delete Snapshot copies, add and delete dataset volumes, provision storage for the dataset, edit provisioning or protection policies
- Prohibited operations: Migration start, migration cancel, migration update, migration cutover, migration cleanup

**Migrate failed** The migration cutover operation failed to bring the destination vFiler unit online. The source vFiler unit is online again and the destination storage system is destroyed.

- Source storage system: Online
- Destination storage : Offline
- Operations permitted: Resize storage, delete Snapshot copies, add and delete dataset volumes, provision storage for the dataset, edit provisioning or protection policies, migration start, migration cancel
- Prohibited operations: Migration cutover, migration cleanup, migration update

**vFiler Unit** The vFiler unit used by the dataset to export data.

### Details area

This area displays detailed information about the migration of the selected dataset.

**Source storage system** The name of the storage system from which the data is migrated.

<b>Destination storage system</b>	The name of the storage system into which the data is migrated.
<b>Source provisioning policy</b>	The name of the provisioning policy applied to the dataset before it was migrated.
<b>Destination provisioning policy</b>	The name of the provisioning policy applied to the dataset after it was migrated.
<b>Volume</b>	The volumes in the dataset.
<b>Lag</b>	The length of time since the most recent successful migration of data to the destination.
<b>State</b>	The state of the volume, SnapVault relationship, or SnapMirror relationship created during the migration.  <b>Initialized</b> The destination storage volume or qtree is not yet initialized or is being initialized.  <b>Snapvaulted</b> The SnapVault relationship is created and the qtree is a SnapVault secondary destination.  <b>Mirrored</b> The destination volume or qtree is in a SnapMirror relationship.  <b>Broken off</b> The destination was in a SnapMirror relationship, but a <code>snapmirror break</code> command made the volume or qtree writable.  This state is reported when the base Snapshot copy is still present in the volume. If the Snapshot copy is deleted, the state is reported as uninitialized while the destination is in the <code>/etc/snapmirror.conf</code> file. The <code>snapmirror resync</code> command restores the mirrored status.  <b>Quiesced</b> SnapMirror is in a consistent internal state and no SnapMirror activity is occurring.  In this state, you can create Snapshot copies with confidence that all destinations are consistent. The <code>snapmirror quiesce</code> command brings the destination into this state. The <code>snapmirror resume</code> command restarts all SnapMirror dataset activities.  <b>Source</b> A <code>snapvault status</code> or <code>snapmirror status</code> command was executed on the primary storage system.  When the destination is on another storage system, its status is unknown and the provisioning application reports the status, "source." This status is also reported for SnapVault relationships when a <code>snapvault status</code> command is executed on secondary

storage systems after the `snapvault restore` command was executed on an associated primary storage system.

<b>Unknown</b>	The destination volume or the volume that contains the destination qtree is in an unknown state.  It might be offline or restricted.
<b>Restoring</b>	SnapVault relationships are being restored.
<b>Status</b>	The status of the volume, SnapVault relationship, or SnapMirror relationship created during the migration.
<b>Idle</b>	The volume has been migrated and is now idle.
<b>Transferring</b>	Data transfer is initiated but not yet finished, or is just finishing.  No data is being transferred.
<b>Pending</b>	The secondary storage system cannot be updated because of a resource issue; the data transfer is retried automatically.
<b>Aborting</b>	A data transfer operation is being aborted and cleaned up.
<b>Migrating</b>	Qtree SnapMirror or volume SnapMirror relationships are being migrated.
<b>Quiescing</b>	The specified volume or qtree is waiting for all existing transfers to complete. The destination is being brought into a stable state.
<b>Resyncing</b>	The specified volume or qtree is being matched with data in the common Snapshot copy.
<b>Waiting</b>	During the migration of qtree SnapMirror or volume SnapMirror relationships, SnapMirror is waiting for a new tape to be put in the tape device.
<b>Syncing</b>	Qtree SnapMirror or volume SnapMirror relationships are being matched with each other.
<b>In_sync</b>	Qtree SnapMirror or volume SnapMirror relationships match each other.
<b>Paused</b>	Qtree SnapMirror or volume SnapMirror relationships are paused.

## Jobs tab

Displays a log of the dataset migration operations initiated on this dataset.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Groups

---

You can use the **Groups** window to add, edit, and delete groups.

- *Command buttons* on page 573
- *Group name* on page 573
- *Details area* on page 573
- *Window customization* on page 573

## Command buttons

- |               |   |
|---------------|---|
| <b>Add</b>    | Starts the <b>Add Group</b> wizard for adding a new group.  |
| <b>Edit</b>   | Opens the properties window for the selected group. From the properties window you can modify the group settings or membership. |
| <b>Delete</b> | Deletes the selected group and all its subgroups, if any.   |

## Group name

Displays the hierarchy of groups, beginning with the default group, Global. You can expand the list to display parent and child groups. You select a group to view its settings.

## Details area

Identifies the group owner, the e-mail address used to alert the owner about events for the group, and the objects that are members of the group.

- |                |   |
|----------------|---|
| <b>Owner</b>   | The name of the person who is to be sent e-mail or pager alerts regarding events for this group.                      |
| <b>E-mail</b>  | One or more e-mail addresses for the person who is to be sent e-mail or pager alerts regarding events for this group. |
| <b>Members</b> | The objects that are members of the group, sorted by object type.   |

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.

- You can click the column display icon  , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data ▶ Resource Pools

---

You can use the **Resource Pools** window to create, view, and modify collections of physical storage resources, called resource pools.

- [Command buttons](#) on page 993
- [Available resource pools list](#) on page 993
- [Resources tab](#) on page 994
- [Space breakout tab](#) on page 994
- [Dependencies tab](#) on page 994
- [Window customization](#) on page 995

When a resource pool is assigned to a dataset, data management applications use the resources in the resource pool to provision storage containers as needed by the dataset and according to the settings defined in policies assigned to the dataset.

## Command buttons

- |               |   |
|---------------|---|
| <b>Add</b>    | Starts a wizard that helps you create a new resource pool.  |
| <b>Edit</b>   | Opens the properties window for the selected resource pool. From the properties window you can modify the settings (Name, Description, Contact, Owner), assigned resources, labels, or space thresholds of an existing resource pool.   |
| <b>Delete</b> | Displays a dialog box that asks you to confirm that you want to delete the selected resource pool. You can either proceed with deleting the selected resource pool or cancel the activity. Deleting a resource pool currently assigned to a dataset also deletes any relationships created in accordance with a policy assigned to that dataset. Deleting a resource pool does <i>not</i> delete the physical resources that were in the resource pool. |

## Available resource pools list

This list displays key property settings and space management information for each of the resource pools.

- |                       |   |
|-----------------------|---|
| <b>Name</b>           | The name assigned to the resource pool.   |
| <b>Total Size</b>     | The total amount of storage space assigned to the resource pool.                            |
| <b>Available Size</b> | The amount of storage space available in the resource pool.                                 |
| <b>Utilization</b>    | The percentage of total storage space being used in the resource pool.                      |
| <b>Owner</b>          | The person who maintains or is responsible for the resource pool, such as an administrator. |

<b>Description</b>	A description that identifies the resource pool.
<b>Time Zone</b>	The time zone you want applied to the resource pool.
	<b>Note:</b> If a resource pool is assigned to a dataset using a Protection Manager policy, the time zone you select can impact the protection schedule. Make sure you understand the potential impact to any of your schedules before changing the Time Zone property.

### Resources tab

<b>Resources</b>	This area displays a tree view of the physical resources assigned to a selected resource pool. The physical resources associated with the selected resource pool are displayed in the expandable Resources list.
------------------	--

### Space breakout tab

The Space breakout tab lists the aggregates assigned to each selected resource pool. If you select one or more items in the list of available resource pools, the aggregates associated with each selected resource pool are displayed in the Space breakout list. If you added a storage system to a selected resource pool, each of its aggregates is listed separately.

<b>Aggregate</b>	The name of the aggregates in the selected resource pool.
<b>Total Size</b>	The total size of the listed aggregate.
<b>Committed Size</b>	The amount of space guaranteed to the volumes contained in the aggregate. This value can be higher than the total size of the aggregate. If you are using the aggregate overcommitment strategy, this value is expressed in KB, MB, GB, or TB.
<b>Available Size</b>	The amount of uncommitted space that is still available in the aggregate. This value is expressed in KB, MB, GB, or TB.
<b>Utilization</b>	The amount of currently used space out of the total size assigned to the aggregate, expressed in percentages.
<b>Datasets</b>	The names of datasets in the selected aggregate. If an aggregate is running out of space, you can use this list to choose which dataset to migrate.
<b>Used Space From Aggregate</b>	The amount of space on the aggregate that is used by the dataset.

### Dependencies tab

The Dependencies tab lists the datasets, if any, that use the selected resource pool and lists whether those datasets are capable of migration. This tab is displayed only when the provisioning license is installed.

<b>Dataset</b>	The datasets with which the selected resource pool is associated.
<b>Migration capable</b>	Whether a listed dataset is configured to be capable of migration.
<b>Remaining number of migration-enabled datasets allowed</b>	The number of additional datasets in the selected resource pool that can be configured for data migration.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data > Unprotected Data > Datasets

---

You can use the **Unprotected Data** window Datasets tab to view datasets that do not have protection policies assigned to them, and you can initiate policy assignments for these datasets.

- [Command button](#) on page 515
- [Datasets list](#) on page 515
- [Window customization](#) on page 515

## Command button

**Protect**      Opens the **Dataset Policy Change** wizard so that you can assign a protection policy to the selected dataset.

## Datasets list

Displays some of the dataset properties that were configured when the dataset was created.

<b>Name</b>	The name of the dataset.
<b>Description</b>	The description of the dataset.
<b>Owner</b>	The owner of the dataset.
<b>Contact</b>	The person to contact for issues with the dataset.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data ► Unprotected Data ► Resources ► Hosts

---

You can use the Hosts button on the Resources tab of the **Unprotected Data** window to view the hosts that contain data that is not assigned to a dataset. You can assign a host containing unprotected data to a dataset. You can also create a new dataset, assign or remove the Ignore property, and view the details about containers holding unprotected data.

- [Command buttons](#) on page 517
- [View Resources buttons](#) on page 517
- [Host Name list](#) on page 518
- [Host content hierarchy area](#) on page 518
- [Host content details area](#) on page 518
- [Window customization](#) on page 519

## Command buttons

<b>Add to new Dataset</b>	Starts the <b>Add Dataset</b> wizard to create a new dataset to which you can add the selected unprotected data.
<b>Add to existing Dataset</b>	Opens a dialog box from which you can select the available dataset to which you want to add the selected unprotected data.
<b>Ignore</b>	Identifies the selected host as an object to be ignored, for purposes of data protection. This allows you to filter the display so that some hosts do not appear in the list of unprotected hosts.  This button also changes the host's Ignored status from No to Yes.
<b>Undo Ignore</b>	Removes the Ignore property from the selected host.  This button also changes the Ignored column status for the selected host from Yes to No.

You can also initiate these actions by right-clicking any host name in this window.

## View Resources buttons

Displays information about all of the unprotected resources available to add to an existing or new dataset.

<b>Hosts</b>	Displays information about hosts that contain data not assigned to a dataset.
<b>Aggregates</b>	Displays the aggregates that contain data not assigned to a dataset.
<b>Volumes</b>	Displays the volumes that contain data not assigned to a dataset.

**Qtrees** Displays the qtrees not assigned to a dataset.

### **Host Name list**

Displays information about hosts that contain data that has not been assigned to a dataset.

**Host Name** The names of a host that contains unprotected data.

**Type** The host type: storage system, vFiler unit, Open Systems SnapVault (displayed as OSSV), or virtual machine.

**Ignored** The Ignore status of each host: Yes (ignored) or No (not ignored).

By default, only the hosts that are not ignored are listed.

### **Host content hierarchy area**

Provides a hierarchical view of the objects contained in the selected host. The hierarchy includes aggregates, volumes, qtrees, non-qtree files, Open Systems SnapVault folders, or virtual machines on the host.

You can select an object in the hierarchy to view details about it.

### **Host content details area**

Provides property details about the objects selected in the host content hierarchy.

**For storage system hosts** Host object properties: Host Name, Host Type, Ignored status

Aggregate object properties: Aggregate Name, Total Size

Volume object properties: Volume Name, Total Size, Unprotected QTrees, Protected QTrees, Total QTrees

Qtree object properties: QTree Name, Used Size

Non-qtree data file object properties: QTree Name, Used Size

**For vFiler hosts** Host object properties: Host Name, Host Type, Ignored status

Volume object properties: Volume Name, Total Size, Unprotected QTrees, Protected QTrees, Total QTrees

Qtree object properties: QTree Name, Used Size

Non-qtree data file object properties: QTree Name, Used Size

**For OSSV (Open Systems SnapVault) hosts** Host object properties: Host Name, Host Type, Ignored status

Directory properties: Directory Name, Full Path

**ESX server host** Host object properties: Host Name, Host Type, Ignored status

**For OSSV (Open Systems SnapVault) ESX server hosts** VM (virtual machine) properties: Virtual machine ID, SnapVault Path, Application Type

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data > Unprotected Data > Resources > Aggregates

---

You can use the Aggregates button on the Resources tab of the **Unprotected Data** window to view the aggregates that contain data that is not assigned to a dataset. You can assign an aggregate containing unprotected data to a dataset. You can also create a new dataset and view the details about aggregates holding unprotected data.

- [Command Buttons](#) on page 521
- [View Resources buttons](#) on page 521
- [Aggregate Name list](#) on page 521
- [Aggregate content hierarchy area](#) on page 522
- [Aggregate content details area](#) on page 522
- [Window customization](#) on page 522

## Command Buttons

<b>Add to new Dataset</b>	Starts the <b>Add Dataset</b> wizard to create a new dataset to which you can add the selected unprotected data.
<b>Add to existing Dataset</b>	Opens a dialog box from which you can select the available dataset to which you want to add the selected unprotected data.
<b>Ignore</b>	This button is disabled when the Aggregate button is selected.
<b>Undo Ignore</b>	This button is disabled when the Aggregate button is selected.

## View Resources buttons

Displays information about all of the unprotected resources available to add to an existing or new dataset.

<b>Hosts</b>	Displays information about hosts that contain data not assigned to a dataset.
<b>Aggregates</b>	Displays the aggregates that contain data not assigned to a dataset.
<b>Volumes</b>	Displays the volumes that contain data not assigned to a dataset.
<b>Qtrees</b>	Displays the qtrees not assigned to a dataset.

## Aggregate Name list

Displays information about aggregates that contain data that has not been assigned to a dataset.

<b>Aggregate Name</b>	The name of the aggregate that contains unprotected data.
-----------------------	---

<b>Host</b>	The name of the host to which the aggregate belongs.
<b>Total Size</b>	The total size of the aggregate.
<b>Used Size</b>	The amount of the volume that is currently used.

### **Aggregate content hierarchy area**

Provides a hierarchical view of the objects contained in the selected aggregate. The hierarchy includes volumes and qtrees.

You can select an object in the hierarchy to view details about it.

### **Aggregate content details area**

Provides property details about the objects selected in the aggregate content hierarchy.

- Aggregate object properties: Aggregate Name and Total Size
- Volume object properties: Volume Name, Total Size, Unprotected Qtrees, Protected Qtrees, Total Qtrees
- Qtree object properties: Qtree Name, Used Size
- Non-qtree data file object properties: Qtree Name, Used Size

### **Window customization**

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Unprotected Data > Resources > Volumes

---

You can use the Volumes button on the Resources tab of the **Unprotected Data** window to view the volumes that contain data that is not assigned to a dataset. You can assign volumes containing unprotected data to a dataset. You can also create a new dataset and view the details about volumes holding unprotected data.

- [Command buttons](#) on page 523
- [View Resources buttons](#) on page 523
- [Volume Name list](#) on page 523
- [Volume content hierarchy area](#) on page 524
- [Volume content details area](#) on page 524
- [Window customization](#) on page 524

## Command buttons

<b>Add to new Dataset</b>	Starts the <b>Add Dataset</b> wizard to create a new dataset to which you can add the selected unprotected data.
<b>Add to existing Dataset</b>	Opens a dialog box from which you can select the available dataset to which you want to add the selected unprotected data.
<b>Ignore</b>	This button is disabled when the Volumes button is selected.
<b>Undo Ignore</b>	This button is disabled when the Volumes button is selected.

## View Resources buttons

Displays information about all of the unprotected resources available to add to an existing or new dataset.

<b>Hosts</b>	Displays information about hosts that contain data not assigned to a dataset.
<b>Aggregates</b>	Displays the aggregates that contain data not assigned to a dataset.
<b>Volumes</b>	Displays the volumes that contain data not assigned to a dataset.
<b>Qtrees</b>	Displays the qtrees not assigned to a dataset.

## Volume Name list

Displays information about volumes that contain data that have not been assigned to a dataset.

<b>Volume Name</b>	The name of the volume that contains unprotected data.
<b>Aggregate</b>	The name of the aggregate to which the volume belongs.

<b>Host</b>	The name of the host to which the volume belongs.
<b>Total Size</b>	The total size of the volume.
<b>Used Size</b>	The amount of the volume that is currently used.
<b>Unprotected Qtrees</b>	The number of unprotected qtrees contained within the volume.

### **Volume content hierarchy area**

Provides a hierarchical view of the objects contained in the selected volume. The hierarchy includes qtrees and nonqtree data.

You can select an object in the hierarchy to view details about it.

### **Volume content details area**

Provides property details about the objects selected in the volume content hierarchy.

Volume object properties: Volume Name, Total Size, Unprotected Qtrees, Protected Qtrees, Total Qtrees

Qtree object properties: Qtree Name, Used Size

Nonqtree data file object properties: Qtree Name, Used Size

### **Window customization**

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Unprotected Data > Resources > Qtrees

---

You can use the Qtrees button on the Resources tab of the **Unprotected Data** window to view the qtrees that contain data that is not assigned to a dataset. You can assign a qtree to a dataset or create a new dataset. You can also view details about qtrees holding unprotected data.

- [Command buttons](#) on page 525
- [View Resources buttons](#) on page 525
- [Qtree Name list](#) on page 525
- [Window customization](#) on page 526

## Command buttons

<b>Add to new Dataset</b>	Starts the <b>Add Dataset</b> wizard to create a new dataset to which you can add the selected unprotected data.
<b>Add to existing Dataset</b>	Opens a dialog box from which you can select the available dataset to which you want to add the selected unprotected data.
<b>Ignore</b>	This button is disabled when the Qtrees button is selected.
<b>Undo Ignore</b>	This button is disabled when the Qtrees button is selected.

## View Resources buttons

Displays information about all of the unprotected resources available to add to an existing or new dataset.

<b>Hosts</b>	Displays information about hosts that contain data not assigned to a dataset.
<b>Aggregates</b>	Displays the aggregates that contain data not assigned to a dataset.
<b>Volumes</b>	Displays the volumes that contain data not assigned to a dataset.
<b>Qtrees</b>	Displays the qtrees not assigned to a dataset.

## Qtree Name list

Displays information about qtrees that contain data that have not been assigned to a dataset.

<b>Qtree Name</b>	The name of the qtree that contains unprotected data.
<b>Volume</b>	The name of the volume to which the qtree belongs.
<b>Host</b>	The name of the host to which the qtree belongs.
<b>Used Size</b>	The amount of used space in the qtree.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Unprotected Data > External Relationships

You can use the **Unprotected Data** window External Relationships tab to view information about the SnapVault and SnapMirror relationships discovered by DataFabric Manager that are not yet managed using a dataset and that are not on the Backup Manager ignore list. From the list of relationships, you can select one or more relationships to import into an existing dataset.

- [Command button](#) on page 527
- [External Relationships list](#) on page 527
- [Window customization](#) on page 527

## Command button

<b>Import</b>	Starts the <b>Import Relationships</b> wizard for putting discovered relationships into datasets.
---------------	---

## External Relationships list

Displays information about the SnapVault and SnapMirror relationships that DataFabric Manager discovered and that are not yet configured for data protection. The list includes relationships where the source volume, qtree, or Open Systems SnapVault directory is not in a dataset and is not on the Backup Manager ignore list. Source storage system names display in ascending order.

<b>Source</b>	The name of the source volume, qtree, or Open Systems SnapVault host.
<b>Type</b>	The type of relationship that DataFabric Manager discovered: SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Destination</b>	The name of the destination volumes and qtrees to which the source data is copied.
<b>Lag</b>	The age of the mirrored copy, which is the difference between the current time and the timestamp of the Snapshot copy last successfully transferred to the destination.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.

- You can click the column display icon  located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Policies > Protection > Overview

---

You can use the **Protection Policies** window Overview tab to view current protection policies, add new protection policies, or edit or copy existing protection policies.

Protection policies are assigned to datasets and specify the type of protection policy (local backup, remote backup, mirror, disaster recovery capable, or a combination of types), the schedule, the backup retention times, and permissible lag times to implement.

- [Command buttons](#) on page 529
- [Policies list](#) on page 529
- [Graph tab](#) on page 531
- [Dependencies tab](#) on page 532
- [Window customization](#) on page 532

## Command buttons

<b>Add</b>	Starts the <b>Add Protection Policy</b> wizard to create a new protection policy.
<b>Edit</b>	Opens a window that allows you to modify the selected policy.
<b>Copy</b>	Copies a selected policy and displays the copy in the Names list as a "Copy of.." Use this button to make customizable copies of selected existing policies in the Policies list.
<b>Delete</b>	Deletes the selected policies.

## Policies list

Displays the currently configured protection policies. Each policy is listed by name and description. If a disaster recovery license is installed, then a DR capable column indicates whether the policy is disaster recovery capable. This list includes the original preconfigured policies and all user-generated policies that were created by using the Add button or by copying and customizing the originals with the Copy and Edit buttons.

<b>Policies:</b>	The following preconfigured policy types are displayed for all installations of the licensed protection application, whether or not a disaster recovery license is also installed. When a disaster recovery license is installed, additional policies are available.
<b>Not disaster recovery capable</b>	<b>Backup</b> Specifies local backup and remote backup of data in primary storage.

<b>No protection</b>	Specifies no data protection whatever in primary storage.  <b>Note:</b> The property Local Backup Schedule Name for the primary data node is preconfigured as blank and is disabled. However, if you assign and enable a protection schedule for this policy, local backups will be scheduled despite the property type.
<b>Local backups only</b>	Specifies local backup protection only (no remote backup) on primary storage.
<b>Mirror</b>	Specifies mirror-copy protection between primary and secondary storage.
<b>Remote backup only</b>	Specifies remote backup protection only from primary to secondary storage (no local backup on primary storage). This policy is appropriate for protecting data on open systems (that is, Windows, UNIX, or Linux-based primary storage systems).  <b>Note:</b> The property Local Backup Schedule Name for the primary data node is preconfigured as blank and is disabled, which prevents you from assigning and enabling a Local backup schedule on the primary data node if it contains Open Systems SnapVault directories.
<b>Back up, then Mirror</b>	Specifies backup protection from primary storage to secondary and mirror-copy protection between secondary storage and tertiary storage.
<b>Mirror, then back up</b>	Specifies mirror-copy protection between primary and secondary storage and backup protection between secondary and tertiary storage.
<b>Mirror and mirror</b>	Specifies mirror-copy protection from primary storage to two different secondary storage destinations.
<b>Mirror, then mirror</b>	Specifies mirror-copy protection between primary and secondary storage and mirror protection between secondary and tertiary storage.
<b>Mirror and back up</b>	Specifies mirror-copy protection from primary storage to one secondary storage location and also backup protection from primary to another secondary storage location.

<b>Policies: Disaster recovery capable</b>	If the disaster recovery license is installed, the following additional disaster recovery capable preconfigured policy types are displayed.
	For each of these policies, if disaster or mishap disables or destroys primary storage, the disaster recovery capable secondary storage is enabled to take over and provide primary storage function and availability.
<b>DR Back up</b>	Specifies disaster recovery capable local and remote backup of the data in primary storage.
<b>DR Mirror</b>	Specifies disaster recovery capable mirror-copy protection between primary and secondary storage.
<b>DR Back up, then mirror</b>	Specifies disaster recovery capable backup protection from primary storage to secondary and mirror-copy protection between secondary storage and tertiary storage.
<b>DR Mirror, then back up</b>	Specifies disaster recovery capable mirror-copy protection between primary and secondary storage and backup protection between secondary and tertiary storage.
<b>DR Mirror and mirror</b>	Specifies disaster recovery capable mirror-copy protection from primary storage to one secondary storage destination and regular mirror-copy protection to another storage destination.
<b>DR Mirror, then mirror</b>	Specifies disaster recovery capable mirror-copy protection between primary and secondary storage and mirror-copy protection between secondary and tertiary storage.
<b>DR Mirror and back up</b>	Specifies disaster recovery capable mirror-copy protection from primary storage to one secondary storage location and also backup protection from primary to another secondary storage location.

## Graph tab

Displays a diagram of the node and connection components of the selected policy. The diagram might include the following components:

**Note:** For a shortcut to directly edit the properties of a node or connection component for the selected policy, click the node or connection in this diagram.

### Primary Data node



This icon represents the primary data storage node of the selected policy. The default name for this node is *Primary data*. However, it can also have a user-specified name, for example, ABCprimarydata.

### Backup Connection



This icon represents the backup connection component of the selected policy.

### Backup node



This icon along with the backup connection icon represents a backup storage node component of the selected policy. The default name for this node is *Backup*. However, it can also have a user-specified name, for example, ABCsecondarybackup.

### Mirror Connection



This icon represents the mirror connection component of the selected policy.

### Mirror node



This icon along with the mirror connection icon represents the mirror node component of the selected policy. The default name for this node is *Mirror*. However, it can also have a user-specified name, for example, ABCsecondarymirror.

## Dependencies tab

Lists the datasets to which the selected policy is assigned. Also displays the protection status for each of the datasets listed.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.

- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Policies > Protection > Schedules

---

You can use the Schedules tab to add, edit, copy, or delete protection schedules and throttle schedules.

- [Command buttons](#) on page 535
- [Schedules list](#) on page 535
- [Dependencies list](#) on page 535
- [Window customization](#) on page 536

## Command buttons

<b>Add</b>	Starts the <b>Add Schedule</b> wizard for adding a throttle schedule or a daily, weekly, or monthly protection schedule.
<b>Edit</b>	Modifies the configuration of the selected schedule.
<b>Delete</b>	Deletes the selected schedule.
<b>Copy</b>	Copies a selected schedule and displays it in the Schedules list as a "Copy of..".

## Schedules list

Displays a list of all the existing daily, weekly, monthly, and throttle schedules. The following schedule types are displayed.

<b>Daily</b>	A schedule that specifies the times for hourly and daily backup or mirror copy operations over a single 24-hour period. When you assign this schedule to a protection policy, you can assign different retention durations to the Hourly and Daily classes of backup.
<b>Weekly</b>	A schedule that specifies the times for hourly, daily, or weekly backup or mirror copy operations over a seven-day period. It consists of one or more daily schedules applied over that time period. When you assign this schedule to a protection policy, you can assign different retention durations to the Hourly, Daily, and Weekly classes of backup.
<b>Monthly</b>	A schedule that specifies the times for hourly, daily, weekly, or monthly backup and mirror copy operations over a month-long period. It consists of a daily or weekly schedule applied over a month-long period. When you assign this schedule to a protection policy, you can assign different retention durations to the Hourly, Daily, Weekly, and Monthly classes of backup.
<b>Throttle</b>	A schedule that specifies periods of unlimited, limited, or zero network bandwidth availability for the data backup or mirror operations.

## Dependencies list

Lists the policies or other schedules to which the selected schedule has been applied.

## **Window customization**

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Hosts > Storage Systems

---

You can use the **Storage Systems Hosts** window to view detailed information about storage systems discovered by DataFabric Manager. From this window, you can add a storage system to NetApp Management Console, edit the properties on existing storage, and diagnose a storage system's configuration. You can also manage Data ONTAP service licenses.

- [Command buttons](#) on page 1005
- [Storage system host list](#) on page 1005
- [Details tab](#) on page 1006
- [Usage tab](#) on page 1010
- [Paths tab](#) on page 1010
- [Input Relationships tab](#) on page 1010
- [Output Relationships tab](#) on page 1011
- [Window customization](#) on page 1011

## Command buttons

<b>Add</b>	Starts the <b>Add Storage System</b> wizard, which allows you to set up storage system hosts.
<b>Edit</b>	Opens a window in which you can modify the properties of the selected host.
<b>Diagnose</b>	Starts the <b>Diagnose Storage Systems</b> wizard, which allows you to modify some aspects of a storage system's configuration.
	This button is disabled if more than one host is selected in the hosts list.
<b>Refresh</b>	Updates the host list for the selected host.

## Storage system host list

<b>Name</b>	Displays the name of the storage system or vFiler unit as it appears in the DataFabric Manager database.
<b>System Status</b>	Displays the current status of the storage system. Possible values are Online, Offline, and Unknown.  The default monitoring interval is one minute. The interval is specified as the Ping Monitoring Interval in Operations Manager.
	You can use the Options page in Operations Manager to view or change the interval. See the Operations Manager online Help for details.

<b>Login Credentials</b>	Displays the current status of the login credentials that DataFabric Manager uses to log in to the host.  Possible values are Good, Bad, Read Only, Unknown, and Not Applicable. NDMP credentials for vFiler units are designated Not Applicable because DataFabric Manager uses the credentials of the hosting system.
<b>NDMP Status</b>	The Network Data Management Protocol (NDMP) availability of the storage system as of the most recent NDMP monitoring check.  Possible values are Up, Down, and Unknown. The default interval for NDMP monitoring is 30 minutes. You can use the Backup Discovery Options page in Operations Manager to change the NDMP monitoring interval. See the Operations Manager online Help for instructions.
<b>NDMP Credentials</b>	Displays the current status of the Network Data Management Protocol credentials that DataFabric Manager uses to communicate with the host.  Possible values are Good, Bad, Unknown, and Not Applicable. NDMP credentials for vFiler units are always designated Not Applicable because DataFabric Manager uses the credentials of the hosting system. You can use the NDMP Credentials page in Operations Manager to edit the credentials for NDMP discovery. See the Operations Manager online Help for details.

## Details tab

The Details tab has four areas: General, Credentials, Service status, and Licenses.

<b>General</b>	
<b>IP Address</b>	Specifies the IP address associated with the selected storage system.
<b>Model</b>	Displays the model number of this storage system.
<b>Mirrored</b>	Indicates whether the SnapMirror license is enabled on this host. Possible values are Yes and No.
<b>Backup Destination</b>	Indicates whether a SnapVault Secondary license is enabled on this host, making the host a potential destination for backups.  Possible values are Yes and No.
<b>Backup Source</b>	Indicates whether the SnapVaultData ONTAP Primary license is enabled on this host, making the host a potential source of backups.  Possible values are Yes and No.  <b>Note:</b> Other hosts might also be potential backup sources, but the SnapVault Primary licenses for Linux, UNIX, and Windows are installed on the secondary system. This list confirms only

whether the SnapVaultData ONTAP Primary license is enabled on the host.

#### Credentials

	<b>Login User Name</b>	The name that DataFabric Manager uses to log in to the selected host.
	<b>NDMP User Name</b>	The name that DataFabric Manager uses to log in to the selected host by using NDMP.

#### Service status

<b>NFS</b>	Indicates whether the Network File System (NFS) service is Up or Down.
<b>CIFS</b>	Indicates whether the Common Internet File System (CIFS) service is Up or Down.
<b>iSCSI</b>	Indicates whether the iSCSI service is Up or Down.
<b>FC</b>	Indicates whether the Fibre Channel (FC) protocol service is Up or Down.

#### Licenses

The following licenses each enable a service of Data ONTAP.

You must enter a software license code on the storage system to enable the corresponding service. You do not need to indicate which license the code enables. The code is matched automatically to the appropriate service license.

<b>SnapMirror</b>	You install the SnapMirror licenses on both the source and destination storage systems for the mirror-copied data.  If the source and destination volumes are on the same system, only one license is required. SnapMirror replicates data to one or more networked storage systems. SnapMirror updates the mirror-copied data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on nonproduction systems, online data migration, and so on. You can also enable the SnapMirror license to use Qtree SnapMirror for backup.
-------------------	--

#### SnapVault Data ONTAP Secondary

You install the SnapVault Secondary license on storage systems hosting the backups of protected data.  
  
SnapVault creates backups of data stored on multiple primary storage systems and copies the backups to a secondary storage system. If data loss or corruption occurs, backed-up data can be restored to a primary or open storage system with little of the downtime and uncertainty associated with conventional tape backup and restore operations.

<b>SnapVault Data ONTAP Primary</b>	You install the SnapVault Data ONTAP Primary license on storage systems running Data ONTAP that contain host data to be backed up.
<b>SnapVault Windows Primary</b>	You install the SnapVault Windows Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a Windows-based primary storage system running the Open Systems SnapVault agent.  A Windows-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>SnapVault Windows Open File Manager</b>	You install the SnapVault Open File Manager license on a <i>secondary</i> storage system to enable the backup of open files on Windows primary storage systems running the Open Systems SnapVault agent.  You must install the SnapVault Windows Primary license and the SnapVault Data ONTAP Secondary license on the secondary storage system before installing the SnapVault Open File Manager license.
<b>SnapVault UNIX Primary</b>	You install the SnapVault UNIX Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a UNIX-based primary storage system (AIX, HP-UX, or Solaris) running the Open Systems SnapVault agent.  A UNIX-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>SnapVault Linux Primary</b>	You install the SnapVault Linux Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a Linux-based primary storage system running the Open Systems SnapVault agent.  A Linux-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>NearStore Option</b>	The NearStore license enables your storage system to use transfer resources as conservatively as if it were optimized as a backup system.  This approach is useful when the storage system on which you want to store backed-up data is not a system optimized for storing backups, and you want to minimize the number of transfer resources the storage system requires. Storage systems using the NearStore license must meet the following criteria: <ul style="list-style-type: none"><li>• The storage system must be a FAS30xx , FAS31xx series , or FAS60xx system.</li><li>• The version of Data ONTAP software must be 7.1 or later.</li></ul>

	<ul style="list-style-type: none"><li>• If you plan to use the SnapVault service, the storage system must have a SnapVault secondary license enabled.</li></ul>
<b>Deduplication</b>	The deduplication license enables you to consolidate blocks of duplicate data into single blocks so that you can store more information using less storage space.  The storage system must have the Deduplication license enabled. If you want to run deduplication on FAS platforms, the NearStore personality license must also be enabled. Monitoring of the volume-level deduplication option is done as part of the core license.
<b>SnapMirror Sync</b>	The SnapMirror Sync license enables you to replicate data to the destination as soon as it is written to the source volume.  SnapMirror Sync is a feature of SnapMirror.
<b>FCP</b>	Fibre Channel (FC) protocol is a licensed service on the storage system that enables you to export LUNs and transfer block data to hosts using the SCSI protocol over a Fibre Channel fabric.
<b>CIFS</b>	Common Internet File System (CIFS) protocol is a licensed service for remote file access that runs over TCP/IP on the Windows operating system.  CIFS enables application access and file sharing across the Internet.
<b>NFS</b>	Network File System (NFS) is client/server application that runs over TCP/IP on the UNIX operating system.  NFS enables application access and file sharing across the Internet.
<b>iSCSI</b>	The iSCSI protocol is a licensed service on the storage system that enables you to transfer block data to hosts using the SCSI protocol over TCP/IP.  iSCSI supports Gigabit Ethernet and is often used in a SAN environment.
<b>MultiStore</b>	The MultiStore license enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems, called vFiler units, on the network.  Be sure that the host on which you intend to install the MultiStore license is running Data ONTAP 6.5 or later.

## Usage tab

The Usage tab provides information about the aggregates, volumes, and qtrees that are associated with any host selected from the host list.

**Resource Type** Displays a tree of the storage system and the aggregates, volumes, and qtrees on that system.

You can also select either aggregates, volumes, or qtrees to narrow the list of resources associated with the storage system that you selected.

**Dependencies** Displays the name of the resource pool or datasets associated with the storage system, aggregate, or volume selected in the Resource Type menu.

## Paths tab

The Paths tab provides information about data that is moving into and out of host paths on the selected storage system. You can use this information to identify dependencies on a selected storage system, aggregate, volume, or qtree.

**Data coming into host path** Displays an expandable list of locations from which data is being backed up or mirror-copied to the selected host path.

**Host path** Displays the host path for which incoming and outgoing data is shown.

You can view the flow of data into and out of the storage system as a whole or expand the list to select a specific aggregate, volume, or qtree and view the flow of data through the selected path. Using the Resource Type menu, you can also select aggregates, volumes, or qtrees to narrow down the listing of resources associated with the storage system you selected.

**Data coming out of host path** Displays an expandable list of locations to which data is being backed up or mirror-copied from the selected host path.

## Input Relationships tab

This tab displays information about systems that send backup or mirror-copy data to the selected system.

You can use this information to identify dependencies on a selected storage system before shutting the system down for maintenance or to assess the impact of an outage.

**Lag Status** Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.

**Lag** Displays the time elapsed since the last successful backup or mirror-copy update.

**Source** Displays the location of the backup or mirror-copy data that is being sent to the selected system.

<b>Type</b>	Displays the type of relationship that the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	Displays the name of the dataset to which the incoming data belongs.
<b>Destination</b>	Displays where the incoming data is being stored on the selected storage system.

### Output Relationships tab

This tab displays information about systems that receive backup or mirror-copy data from the selected system.

You can use this information to identify dependencies on a selected storage system before shutting the system down for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	Displays the time elapsed since the last successful backup or mirror-copy update.
<b>Source</b>	Displays the location of data on the system that is being backed up or mirror-copied to a secondary system.
<b>Type</b>	Displays the type of relationship the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	Displays the name of the dataset to which the outgoing data belongs.
<b>Destination</b>	Displays where the outgoing data is being stored on the destination system.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Hosts > OSSV

---

You can use the **OSSV Hosts** window to add, edit, or diagnose the Open Systems SnapVault hosts that are discovered by DataFabric Manager. From this window, you can manage host login or NDMP credentials and Data ONTAP service licenses. You can also start, stop, and refresh Open Systems SnapVault hosts.

- [\*Command buttons\*](#) on page 545
- [\*Host list\*](#) on page 545
- [\*Details tab\*](#) on page 546
- [\*Paths tab\*](#) on page 547
- [\*Window customization\*](#) on page 548

## Command buttons

<b>Add</b>	Starts the <b>Add OSSV Host</b> wizard, which allows you to set up Open Systems SnapVault hosts.
<b>Edit</b>	Opens a window in which you can modify the properties of the selected host.
<b>Diagnose</b>	Opens the <b>Diagnose Storage Systems</b> wizard, which allows you to modify some aspects of a storage system's configuration.
This button is disabled if more than one host is selected in the hosts list.	
<b>Start</b>	Starts the Open Systems SnapVault agent on the selected system.
<b>Stop</b>	Stops the Open Systems SnapVault agent on the selected system.
<b>Refresh</b>	Updates the host list for the selected host.

## Host list

Displays information about Open Systems SnapVault hosts discovered by DataFabric Manager.

<b>Name</b>	Displays the name of the host as it appears in the DataFabric Manager database.
<b>System Status</b>	<p>Displays the current status of the host.</p> <p>Possible values are Up, Down, and Unknown. The default monitoring interval is one minute. The interval is specified as the Ping Monitoring Interval in Operations Manager. You can use the Options page in Operations Manager to view or change the interval. See the Operations Manager online Help for details.</p>

**Host Agent Status** Displays the current status of NetApp Host Agent .

Possible values are Detected and Not Detected.

**Note:** There is no Open Systems SnapVault plug-in for Solaris, so the NetApp Host Agent cannot communicate with the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console.

**Host Agent Credentials** Displays the current status of the login credentials that DataFabric Manager uses to log in to NetApp Host Agent .

Possible values are Good, Bad, and Unknown.

**NDMP Status** Displays the current status of the Network Data Management Protocol (NDMP).

Possible values are Up, Down, and Unknown.

**NDMP Credentials** Displays the current status of the NDMP credentials that DataFabric Manager uses to communicate with the host.

Possible values are Good, Bad, and Unknown.

## Details tab

The details tab reflects information about the host selected in the hosts list. This tab contains three sections: General, Host Agent Settings, and NDMP Settings.

### General

<b>Host Name</b>	The name of the currently selected host.
<b>IP Address</b>	The IP address associated with the selected host.
<b>System Status</b>	Whether the status of the Open Systems SnapVault host is Up, Down, or Unknown.
<b>OS</b>	The operating system running on the host.
<b>Version</b>	The version of the operating system running on the host.

### Host Agent Settings

<b>Status</b>	Whether NetApp Host Agent is Detected or Not Detected on the assigned port.
<b>Credentials Status</b>	Whether the status of the credentials for NetApp Host Agent on the selected host is Good, Bad, or Unknown.
<b>User Name</b>	The name that DataFabric Manager uses to log in to NetApp Host Agent on the selected host.

	<b>Port</b>	The port that DataFabric Manager uses to log in to NetApp Host Agent .  The default port number is 4092.
<b>NDMP Settings</b>	<b>Status</b>	Whether the status of the data management protocol for the selected host is Up, Down, or Unknown.
	<b>Credentials Status</b>	Whether the status of the data management protocol for the selected host is Good, Bad, or Unknown.
	<b>User Name</b>	The name that DataFabric Manager uses to log in to the selected host by using NDMP.
	<b>Port</b>	The port that DataFabric Manager uses to log in to a host running the Open Systems SnapVault agent.  The default port number is 10000. This port is not valid for other types of host.

## Paths tab

The Path area provides a way to browse host directories and to view which datasets the directories are assigned to, if any.

Select any item in the pane to display information about that item.

**Note:** The paths on an Open Systems SnapVault client are filtered using the Operations Manager Backup Discovery property, Directories to Ignore. If a path matches the settings specified for this property, the path is ignored and new directories in that path are not protected automatically. For more information, see the Operations Manager online Help.

<b>Path</b>	The path of the currently selected directory or file.
<b>Status</b>	The protection status of the currently selected path. Possible values are as follows:
<b>Protected</b>	The data is being protected according to policy (normal).
<b>Unprotected</b>	The data is not protected by a policy (warning).
<b>Uninitialized</b>	There are no backups of the data (normal).
<b>Protection suspended</b>	An administrator has requested that all scheduled backups be canceled until the administrator requests that the backups be resumed (warning).
<b>Job failure</b>	An error occurred while the data was being protected (warning).

**Lag warning** The dataset is nearing the lag threshold (warning).

**Lag error** The protection lag has exceeded the configured lag threshold (error).

**Datasets** The datasets to which the directory is assigned, if any.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Hosts > vFiler Units

---

You can use the **vFiler Units** window to view detailed information about vFiler units discovered by DataFabric Manager. From this window you can add vFiler units to or delete them from the NetApp Management Console host list. You can also access the Details tab, Paths tab, and the Relationships tabs for vFiler units.

- [Command buttons](#) on page 1023
- [vFiler units list](#) on page 1024
- [Details tab](#) on page 1026
- [Network Settings tab](#) on page 1027
- [Paths tab](#) on page 1028
- [Input Relationships tab](#) on page 1029
- [Output Relationships tab](#) on page 1029
- [Migration tab](#) on page 1030
- [Window customization](#) on page 1031

## Command buttons

The migration command buttons are disabled when a vFiler unit migration is in progress.

<b>Add</b>	Starts the <b>Add vFiler Unit</b> wizard, which allows you to create and to optionally configure vFiler units.  You can choose to create the vFiler unit by using the Add button and then configure it later by using the Setup button.
<b>Setup</b>	Starts the <b>Setup vFiler Unit</b> wizard, which allows you to configure or modify an existing vFiler unit.
<b>Delete</b>	Deletes the selected vFiler unit from the NetApp Management Console vFiler list.
<b>Start migration</b>	Initiates the first phase of a vFiler unit migration by starting the <b>vFiler Unit Migration</b> wizard, which begins a baseline transfer.
<b>Update</b>	Performs an on demand update of the SnapMirror relationships that were created as part of the "Start migration" operation. This button is enabled only when the "Start migration" operation has finished for the selected vFiler unit.
<b>Cutover</b>	Initiates the second phase of a migration, which performs a cutover (in other words, switches the source from the old storage from which the data is served to the new storage destination). This button is enabled only when the migration start operation has finished for the selected vFiler unit.

<b>Cancel</b>	Cancels the migration in progress for the selected dataset by stopping the migration process and returning the dataset to the status it had before the migration started. All ongoing data transfers for the migration are aborted, and the provisioned destination storage and destination vFiler unit are deleted. (You must manually delete VLANs and IPspaces that were created during the migration process.) This button is enabled during the migration start and update operations.
<b>Cleanup</b>	Initiates the third phase of a migration, which deletes the old storage from which the vFiler unit was migrated. A preview window lists which volumes are to be destroyed as part of the cleanup operation. VLANs and IPspaces used by the source vFiler unit are not automatically destroyed. This button is enabled only when a migration cutover process has finished for the selected vFiler unit.

## vFiler units list

<b>Name</b>	The name of the vFiler unit as it appears in the DataFabric Manager database.
<b>IP address</b>	The IP address associated with the selected vFiler unit.
<b>IP Space</b>	The name of the IPspace, if any, assigned to the vFiler unit.
<b>Hosting Storage System</b>	The name of the storage system that hosts the vFiler unit.
<b>System Status</b>	The current status of the vFiler unit. Possible values are Online, Offline, and Unknown. The default monitoring interval is five minutes. The interval is specified as the Ping Monitoring Interval in Operations Manager. You can use the Options page in Operations Manager to view or change the interval. See the Operations Manager online Help for details.
<b>Migration Status</b>	The status of a migrating source vFiler unit. The description, source storage status, destination storage status, permitted operations, and prohibited operations for each status are described as follows.  <b>Not started</b> The vFiler unit meets the vFiler unit migration requirements. <ul style="list-style-type: none"><li>• Source storage system: Online</li><li>• Destination storage : Not provisioned</li><li>• Operations permitted: All</li><li>• Prohibited operations: Migration cutover, migration update, migrate complete, migration cancel, migration cleanup</li></ul> You can initialize the start migration operation on vFiler units having a "Not started" or "Migrate failed" status.

<b>In progress</b>	Migration of this vFiler unit has started. <ul style="list-style-type: none"><li>Source storage system: Online</li><li>Destination storage : Provisioned for the vFiler unit then offline</li><li>Operations permitted: Migration cancel</li><li>Prohibited operations: Add or delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies</li></ul>
<b>Started, cutover required</b>	The vFiler unit is completely migrated to the destination storage system including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. The data source needs to be switched to the new vFiler unit on the new destination storage system. <ul style="list-style-type: none"><li>Source storage system: Offline</li><li>Destination storage: Online</li><li>Operations permitted: Edit provisioning or protection policies, migration update, migration cutover, migration cancel</li><li>Prohibited operations: Migration cleanup</li></ul>
<b>Migrated, cleanup required</b>	The migration cutover operation is finished and the vFiler unit is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. Old storage needs to be deleted. <ul style="list-style-type: none"><li>Source storage system: Offline</li><li>Destination storage : Online</li><li>Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies, migration cleanup</li><li>Prohibited operations: Migration start, migration cancel, migration update, migration cutover</li></ul>
<b>Migrated with errors</b>	The migration cutover operation successfully performed the switch to the destination storage system. However, a failure occurred during the migration of the backup version, backup relationships, or history for the primary data. You must manually correct the errors. <ul style="list-style-type: none"><li>Source storage system: Offline</li><li>Destination storage : Online</li><li>Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies</li></ul>

- Prohibited operations: Migration start, migration cancel, migration update, migration cutover, migration cleanup

<b>Migrate failed</b>	The migration cutover operation failed to bring the destination vFiler unit online. The source vFiler unit is online again and the destination storage system is destroyed. <ul style="list-style-type: none"><li>• Source storage system: Online</li><li>• Destination storage : Offline</li><li>• Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies, migration start, migration cancel</li><li>• Prohibited operations: Migration cutover, migration cleanup, migration update</li></ul>
-----------------------	--

## Details tab

The Details tab has three areas: General, Service status, and Hosting Storage System Settings.

<b>General</b>	<b>Protocols</b>	Indicates the protocol type associated with the vFiler unit, either CIFS, NFS, or iSCSI.
<b>Mirrored</b>		Indicates whether the SnapMirror license is enabled on the hosting storage system. Possible values are Yes or No.
<b>Backup Destination</b>		Indicates whether a SnapVault Secondary license is enabled on this host, making the host a potential destination for backups. Possible values are Yes or No.
<b>Backup Source</b>		Indicates whether the SnapVault Data ONTAP Primary license is enabled on the hosting storage system, making the host a potential source of backups. Possible values are Yes or No. <b>Note:</b> Other hosts might also be potential backup sources, but the SnapVault Primary licenses for Linux, UNIX, and Windows are installed on the secondary system. This list confirms only whether the SnapVault Data ONTAP Primary license is enabled on the host.

<b>Service status</b>	<b>NFS</b>	Indicates whether the Network File System (NFS) service is Up or Down.
	<b>CIFS</b>	Indicates whether the Common Internet File System (CIFS) service is Up or Down.
	<b>iSCSI</b>	Indicates whether the iSCSI service is Up or Down.
<b>Hosting Storage System Settings</b>	These settings apply to the storage system that is hosting the vFiler unit that you selected in the vFiler list.	
	<b>Host Name</b>	The name that DataFabric Manager uses to log in to the storage system.
	<b>IP Address</b>	The IP address of the hosting storage system that is associated with the selected vFiler unit.
	<b>System Status</b>	Whether the status of the storage system is Online, Offline, or Unknown.
	<b>Login Credentials Status</b>	The current status of the login credentials that DataFabric Manager uses to log in to the hosting storage system. Possible values are Good, Bad, Read Only, Unknown, and Not Applicable.
	<b>NDMP Status</b>	<p>The Network Data Management Protocol (NDMP) availability of the storage system as of the most recent NDMP monitoring check.</p> <p>Possible values are Up, Down, and Unknown. The default interval for NDMP monitoring is 30 minutes.</p> <p>You can use the Backup Discovery Options page in Operations Manager to change the NDMP monitoring interval. See the Operations Manager online Help for instructions.</p>
	<b>NDMP Credentials Status</b>	<p>The current status of the Network Data Management Protocol credentials that DataFabric Manager uses to communicate with the hosting storage system.</p> <p>Possible values are Good, Bad, Unknown, and Not Applicable.</p> <p>You can use the NDMP Credentials page in Operations Manager to edit the credentials for NDMP discovery. See the Operations Manager online Help for details.</p>

## Network Settings tab

This tab provides information about vFiler unit administrative hosts and servers, and network bindings.

<b>Network information area</b>	This area displays information about administrative hosts and servers for a selected vFiler unit.
<b>Administrative host</b>	Indicates the IP address of the administrative host for the selected vFiler unit.
<b>DNS domain name</b>	Indicates the domain name of the DNS server for the selected vFiler unit.
<b>DNS servers</b>	Indicates the IP addresses of DNS servers for the selected vFiler unit.
<b>NIS domain name</b>	Indicates the domain name of the NIS server for the selected vFiler unit.
<b>NIS servers</b>	Indicates the IP addresses of NIS servers for the selected vFiler unit.
<b>CIFS authentication type</b>	Indicates the mode used to authenticate data requests to or from a selected vFiler unit. Values are Active directory or Windows workgroup.
<b>CIFS security style</b>	Indicates the security protocol to be used by a selected vFiler unit. Values are NTFS-only or Multiprotocol.
<b>CIFS workgroup name</b>	Indicates the name of the CIFS Windows workgroup.
<b>Network Bindings</b>	You can use network bindings to bind network cards, protocols, and services.
<b>IP address</b>	The IP address of a network card or port that you have bound to a specific protocol or service.
<b>Network mask</b>	The network mask of a network card or port that you have bound to a specific protocol or service.
<b>Network interface</b>	The protocol or service to which the corresponding IP address is bound.

## Paths tab

The Paths tab displays information about data that is moving into and out of host paths on the selected vFiler unit. You can use this information to identify dependencies on a selected vFiler unit, aggregate, volume, or qtree.

<b>Data coming into host path</b>	A list of locations from which data is being backed up or mirrored to the selected host path.
-----------------------------------	---

<b>Host path</b>	The host path for which incoming and outgoing data is shown for the storage system that is hosting the vFiler unit.
	You can view the flow of data into and out of the storage system as a whole, or you can expand the list to select a specific aggregate, volume, or qtree and view the flow of data through the selected path.
<b>Data coming out of host path</b>	A list of locations to which data is being backed up or mirrored from the selected host path.

### Input Relationships tab

This tab displays information about systems that send backup or mirror data to the storage system that is hosting the vFiler unit.

You can use this information to identify dependencies on a selected storage system before shutting down the system for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	The time elapsed since the last successful backup or mirror update.
<b>Source</b>	The location of the backup or mirror data that is being sent to the selected system.
<b>Type</b>	The type of relationship that the system has with the hosting storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	The name of the dataset to which the incoming data belongs.
<b>Destination</b>	The name of the hosting storage system on which the incoming data is being stored.

### Output Relationships tab

This tab displays information about systems that receive backup or mirror data from the hosting storage system.

You can use this information to identify dependencies on a selected storage system before shutting down the system for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	The time elapsed since the last successful backup or mirror update.
<b>Source</b>	The location of data on the system that is being backed up or mirrored to a secondary system.

<b>Type</b>	The type of relationship the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	The name of the dataset to which the outgoing data belongs.
<b>Destination</b>	The name of the destination system on which the outgoing data is being stored.

### **Migration tab**

This tab displays detailed information about the data migration of the datasets attached to the selected vFiler unit.

<b>Source storage system</b>	The name of the storage system from which the data is migrated.
<b>Destination storage system</b>	The name of the storage system into which the data is migrated.
<b>Migration Status</b>	The same migration status as in the vFiler units list section of this window.
<b>Dataset(s) attached</b>	The datasets to which the selected vFiler unit is attached.
<b>Physical resources</b>	The volumes in the dataset.
<b>Lag</b>	The length of time since the successful migration of data to the destination.
<b>Error</b>	The error that occurred during a migration operation.  The value None indicates that no migration-related error occurred.
<b>State</b>	The state of the volume, SnapVault relationship, or SnapMirror relationship created during the migration.  <b>Uninitialized</b> The destination storage volume or qtree is not yet initialized or is being initialized.  <b>Snapvaulted</b> The SnapVault relationship is created and the qtree is a SnapVault secondary destination.  <b>Mirrored</b> The destination volume or qtree is in a SnapMirror relationship.  <b>Broken off</b> The destination was in a SnapMirror relationship, but a <code>snapmirror break</code> command made the volume or qtree writable.  This state is reported when the base Snapshot copy is still present in the volume. If the Snapshot copy is deleted, the state is reported as uninitialized while the destination is in the <code>/etc/snapmirror.conf</code> file. The <code>snapmirror resync</code> command restores the mirrored status.

<b>Quiesced</b>	SnapMirror is in a consistent internal state and no SnapMirror activity is occurring.
	In this state, you can create Snapshot copies with confidence that all destinations are consistent. The <code>snapmirror quiesce</code> command brings the destination into this state. The <code>snapmirror resume</code> command restarts all SnapMirror activities.
<b>Source</b>	A snapvault status or snapmirror status command was executed on the primary storage system.
	When the destination is on another storage system, its status is unknown and the provisioning application reports the status, "source." This status is also reported for SnapVault relationships when a <code>snapvault status</code> command is executed on secondary storage systems after the <code>snapvault restore</code> command was executed on an associated primary storage system.
<b>Unknown</b>	The destination volume or the volume that contains the destination qtree is in an unknown state.
	It might be offline or restricted.
<b>Restoring</b>	SnapVault relationships are being restored.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Events window

---

You can use the **Events** window to monitor, acknowledge, and delete events.

- [Command buttons](#) on page 559
- [View Events buttons](#) on page 559
- [Events list](#) on page 559
- [Details area](#) on page 561
- [Window customization](#) on page 561

## Command buttons

**Acknowledge** Acknowledges the selected events; your user name and the time are entered in the Event List for the selected events. When you acknowledge an event, you take responsibility for managing that event.

**Delete** Deletes the selected events from the Events summary list, so that the deleted events are not considered when calculating the status of a dataset, volume, and so forth. To view a list of deleted events, you can use the Operations Manager interface.

## View Events buttons

These filter buttons specify the range of events displayed in the events list.

- |                |  |
|----------------|--|
| <b>1 Day</b>   | Displays events that occurred today.   |
| <b>1 Week</b>  | Displays events that occurred in the last seven days.                              |
| <b>1 Month</b> | Displays events that occurred in the last 30 days.                                 |
| <b>All</b>     | Displays all events related to the NetApp Management Console client you are using. |

**Note:** On very large or very busy systems, the **Events** window might be unresponsive for long periods while loading **1 Month** or **All** data. If the application appears unresponsive for these large lists, select a shorter time period (such as **1 Day**).

## Events list

Displays a list of the events that occurred. The list of events is updated dynamically, as events occur. You can select an event to see the details for that event.

**Note:** The list of events that can be downloaded is limited to 25,000 records.

<b>Severity</b>	Displays the severity type. The default events list includes this column, which can be filtered to show a severity type and all severity types worse than the selected one.
The severity types are as follows.	
<b>Unknown</b>	The event is in an unknown transitory state.
<b>Unmanaged</b>	The event source is not managed by the protection or provisioning applications. No action is required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds. No action is required.
<b>Information</b>	The event is a normal occurrence. No action is required.
<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Error</b>	The event source is still performing, but corrective action is required to avoid service disruption.
<b>Critical</b>	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
<b>Emergency</b>	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
<b>Event</b>	Displays the event names. You can select an event to display the event details. The default events list includes this column.
<b>Triggered</b>	Displays the time and date the event was issued. The default events list includes this column.
<b>Acknowledged By</b>	Displays the user name of the person who acknowledged the event. The field is blank if the event is not acknowledged. The default events list includes this column.
<b>Acknowledged Time</b>	Displays the time the event was acknowledged. The field is blank if the event is not acknowledged. The default events list includes this column.
<b>Source</b>	Displays the full object name that triggered the event. The default events list includes this column.
<b>Deleted By</b>	Displays the user name that deleted the event. This column is not displayed by default.
<b>Deleted Time</b>	Displays the time the event was deleted. This column is not displayed by default.

## Details area

The area below the event list displays detailed information about the selected event, as follows:

<b>Event</b>	The event name.
<b>Source</b>	The full object name to which the event is associated.
<b>Source Type</b>	The object type that triggered the event.
<b>Severity</b>	The severity type of the event.
<b>About</b>	Additional description of the event.
<b>Triggered</b>	The time and date the event occurred.
<b>Acknowledged</b>	Whether the event was acknowledged and by whom.
<b>Deleted</b>	Whether the event was deleted from the Events list.
<b>Condition</b>	A description of the condition that triggered the event.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Alarms window

---

You can use the **Alarms** window to monitor and configure alarms. You can also disable and enable alarms.

- [Command buttons](#) on page 563
- [Alarms list](#) on page 563
- [Details area](#) on page 564
- [Window customization](#) on page 565

## Command buttons

<b>Add</b>	Starts the <b>Add Alarm</b> wizard.
<b>Edit</b>	Opens the <b>Properties</b> sheet for modifying the configuration of the selected alarm.
<b>Delete</b>	Deletes the selected alarm.
<b>Test</b>	Tests the selected alarm by sending a test notification to all recipients.

## Alarms list

Displays a list of the currently configured alarms. The list is updated dynamically when the status changes.

<b>Event</b>	If the alarm is configured for a specific event, shows the event that triggers the alarm. Or, if the alarm is configured for an event class, shows the event class for which all events that occur in that class trigger the alarm.
<b>Severity</b>	If the alarm is configured for a severity type, shows the severity type that marks the lowest severity level that triggers the alarm. The default alarms list includes this column, which can be filtered to show a severity type and all severity types worse than the selected one.
<b>Unknown</b>	The event is in an unknown transitory state.
<b>Unmanaged</b>	The event source is not managed by the protection or provisioning applications. No action is required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds. No action is required.
<b>Information</b>	The event is a normal occurrence. No action is required.

<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Error</b>	The event source is still performing, but corrective action is required to avoid service disruption.
<b>Critical</b>	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
<b>Emergency</b>	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
<b>Group</b>	Shows the resource group the alarm is associated with. The default group is Global. You can associate an alarm with any resource group that is defined.
<b>Enabled</b>	Shows whether the alarm is currently enabled (selected) or disabled (not selected). The default is enabled.
<b>Details area</b>	
Displays detailed information about the selected alarm.	
<b>Event class</b>	Shows the class of events for which the alarm is configured. Event classes can only be selected; they are defined using Protection Manager, Provisioning Manager, or Operations Manager.
<b>Repeat Notify (min)</b>	Specifies whether an alarm notification is repeated until the event is acknowledged and how often the notification is repeated. The default is no repeat notification.
<b>minutes value displayed</b>	Repeats the event notification at the interval specified, until the event is acknowledged.
<b>no minutes value displayed</b>	Event notification is sent only once and is not repeated.
<b>Active range</b>	Specifies the time during which the alarm can be triggered. If a specific event or an event of a specified severity type occurs at a time at which the alarm is not active, no event notification occurs. For example, you might want an event notification to occur only when a specific administrator is available.
<b>Start</b>	Specifies the time at which the alarm becomes active, based on the time zone of the storage set to which the event notification applies.
<b>Stop</b>	Specifies the time at which the alarm becomes inactive, based on the time zone of the storage set to which the event notification applies.

**Recipients** Specifies where the event notification is to be sent.

**E-mails**

- |  |   |
|--|---|
| <b>Administrators</b><br><b>Non-Administrators</b> | Shows the administrators who will receive the event notification by e-mail.<br>Shows other users who will receive the event notification by e-mail. |
|--|---|

**Pagers**

- |  |   |
|--|---|
| <b>Administrators</b><br><b>Non-Administrators</b> | Shows the administrators who will receive an event notification message at a pager e-mail address.<br>Shows other users who will receive an event notification message at a pager e-mail address. |
|--|---|

**Traps**

- Shows the servers that contain an SNMP trap listener to receive the event notification.

**Script**

- |                                       |  |
|---------------------------------------|--|
| <b>Script</b><br><b>Run script as</b> | Shows the full path name of a script that is executed when an alarm occurs.<br>Shows the user name to be used to run the script. |
|---------------------------------------|--|

For more information about SNMP traps, see the *Operations Manager Administration Guide*.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

**Related information**

*Operations Manager Administration Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Data ▶ Jobs

---

You can use the **Jobs** window to view status information for jobs initiated within NetApp Management Console .

- [Command button](#) on page 1041
- [View Jobs buttons](#) on page 1041
- [Jobs list](#) on page 1042
- [Completed Steps](#) on page 1045
- [Event description](#) on page 1045
- [Window customization](#) on page 1045

## Command button

**Cancel** Stops the selected jobs. You can select multiple jobs and cancel them simultaneously. This button is active only when the selected jobs are in progress.

## View Jobs buttons

These buttons specify the range of jobs displayed in the summary list.

**1 Day** Displays all jobs that were started between midnight of the previous day and now. (Jobs that were started before this period are not included even if they are still running.) This period can cover up to 47 hours and 59 minutes.

For example, if you click 1 Day at 15:00 on February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) on February 13 to the current time on February 14. This list covers the full day of February 13 plus the partial current day of February 14.

**1 Week** Displays all jobs that were started between midnight of the same day in the previous week (seven days ago) and now. (Jobs that were started before this period and are still running are not included.) This period can cover up to seven days, 23 hours, and 59 minutes.

For example, if you click 1 Week at 15:00 on Thursday, February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) the previous Thursday (February 7) to the current time on February 14. This list covers seven full days plus the partial current day.

**1 Month** Displays all jobs that were started between midnight of the same day in the previous month and now. (Jobs that were started before this period and are still running are not included.) This period can cover from 28 through 32 days, depending on the month.

For example, if you click 1 Month at 15:00 on Thursday, February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) on January 14 to the current time on February 14.

**All** Displays all jobs.

**Note:** On very large or very busy systems, the **Data > Jobs** window might be unresponsive for long periods while loading 1 Month or All data. If the application appears unresponsive for these large lists, select a shorter time period (such as 1 Day).

## Jobs list

Displays a list of the jobs that occurred. The list of jobs is updated dynamically, as jobs start or finish. You can customize the display using the filtering and sorting options in the jobs list.

**Note:** The lists of jobs that can be downloaded is limited to 25,000 records.

**Job Type** The type of job, which is determined by the policy assigned to the dataset or by the direct request initiated by a user. The default jobs list includes this column. The job types are as follows:

**Create relationship** A protection relationship create operation based on SnapMirror technology.

**Delete Snapshot copies** A job that deletes Snapshot copies of volumes of a dataset.

**Delete storage** A job that deletes a volume, qtree, or LUN from the storage system.

**Attention:** This operation will destroy the data in the deleted volume, qtree, or LUN. This operation cannot be reversed.

**Destroy relationship** A protection relationship delete operation based on SnapMirror technology.

**Failover** A dataset failover operation of a primary node to a disaster recovery node. Applies only if the dataset is enabled for disaster recovery.

**Local backup** A local scheduled backup protection operation based on Snapshot technology.

**Local backup confirmation** A local scheduled backup protection operation based on Snapshot technology. Applies if a dataset is an

	application-generated dataset and if the application is responsible for creating local backups.
<b>Mirror</b>	A scheduled protection mirror operation based on SnapMirror technology.
<b>On-demand protection</b>	A backup or mirror operation that is initiated by the Protect Now button in the <b>Datasets</b> window. The types of tasks performed are determined by the policy configured for the dataset.
<b>Provision</b>	A job that provisions containers into a dataset based on the associated policy and dataset attributes.
<b>Remote backup</b>	A scheduled backup to secondary storage based on SnapVault technology.
<b>Resize storage</b>	A job that changes the storage size or quota limit. If the selected container is a volume, this job type changes the size, Snapshot reserve, and maximum size of the volume. If the selected container is a qtree, this job type changes the quota limit of the qtree.
<b>Restore</b>	A protection data restore job that is initiated by the Restore button in the <b>Datasets</b> window.
<b>Dedupe volume</b>	A deduplication space savings operation initiated on a selected volume.
<b>Undedupe volume</b>	A deduplicated volume has been converted to a normal volume.
<b>Start migration</b>	A job that begins migrating a dataset or vFiler unit to a new storage system.
<b>Cancel migration</b>	A job that cancels a dataset or vFiler unit migration.
<b>Cleanup migration</b>	A job that deletes the old storage after a dataset or vFiler unit migration cutover.
<b>Cutover</b>	A job that switches the source of a dataset or vFiler unit from the old storage system to a new storage system.
<b>Migration update</b>	A job that updates the SnapMirror relationships that were created as part of the migration start operation.
<b>Relinquish migration</b>	A job that relinquishes the migration capability of a dataset.
<b>Dataset</b>	The name of the dataset on which the job was started. The default jobs list includes this column.

<b>vFiler Unit</b>	The name of the vFiler unit on which the job was started. The default jobs list includes this column if the provisioning license is installed.
<b>Start</b>	The date and time the job was started. The default jobs list includes this column.
<b>Job Status</b>	The running status of the job. The default jobs list includes this column. The progress options are as follows:
<b>Failed</b>	All tasks in the job failed.
<b>Partially Failed</b>	One or more of the tasks in the job failed and one or more of the tasks completed successfully.
<b>Succeeded</b>	All tasks completed successfully.
<b>Running</b>	The job is currently running.
<b>Running with Error</b>	The job is currently running but with an error.
<b>Queued</b>	The job is not running yet. However, it is scheduled to run after other provisioning jobs on the same dataset are completed.
<b>Canceled</b>	The job stopped because the Cancel button was clicked to stop the job before it was completed.
<b>Canceling</b>	The Cancel button was clicked and the job is in the process of stopping.
<b>End</b>	The date and time the job ended. The default jobs list includes this column.
<b>ID</b>	The identification number of the job.  The ID column is not displayed in the jobs list by default. The job identification number is unique and is assigned by the server when it starts the job. You can search for a particular job by entering the job identification number in the text box provided by the column filter.
<b>Bytes Transferred</b>	The amount of data (in megabytes or gigabytes) that was transferred during the job, as reported by DataFabric Manager. This column is not displayed in the jobs list by default.  <b>Note:</b> This number is an approximation and does not reflect an exact count; it is always less than the actual number of bytes transferred. For short jobs (jobs that take a short time to complete), no data transfer size is reported.
<b>Policy</b>	The name of the policy associated with the job. This column is not displayed in the jobs list by default.
<b>Source Node</b>	The name of the storage resource that contains the data being protected. This column is not displayed in the jobs list by default.

<b>Destination Node</b>	The name of the storage resource to which the data is transferred during the job. This column is not displayed in the jobs list by default.
<b>Submitted By</b>	The policy that automatically started the job or the user name of the person who started the job. This column is not displayed in the jobs list by default.
<b>Description</b>	A description of the job taken from the policy configuration or the job description entered when the job was manually started. This column is not displayed in the jobs list by default.

## Completed Steps

Displays detailed information about each task in the selected job. You can select a step to see its details.

<b>Time stamp</b>	The date and time the step was completed.
<b>Step</b>	A description of the step: for example, Start, in Progress, or End.
<b>Result</b>	The result of the step. Result options are as follows:
<b>Error</b>	The step failed.
<b>Warning</b>	The step succeeded but with a possible problem.
<b>Retry</b>	The provisioning engine has performed undo and retry operations.
<b>Normal</b>	The step succeeded.

## Event description

Displays detailed information about events and errors that occurred during each step of a job. The information displayed in this area includes much of the same information that is provided in the columns of the Details area. However, it also includes the unique items Job Description and Error Message.

To view the details, select an item from the jobs list, then select an item from the Completed Steps list.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.

- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data > Groups

---

You can use the **Groups** window to add, edit, and delete groups.

- *Command buttons* on page 573
- *Group name* on page 573
- *Details area* on page 573
- *Window customization* on page 573

## Command buttons

- |               |   |
|---------------|---|
| <b>Add</b>    | Starts the <b>Add Group</b> wizard for adding a new group.  |
| <b>Edit</b>   | Opens the properties window for the selected group. From the properties window you can modify the group settings or membership. |
| <b>Delete</b> | Deletes the selected group and all its subgroups, if any.   |

## Group name

Displays the hierarchy of groups, beginning with the default group, Global. You can expand the list to display parent and child groups. You select a group to view its settings.

## Details area

Identifies the group owner, the e-mail address used to alert the owner about events for the group, and the objects that are members of the group.

- |                |   |
|----------------|---|
| <b>Owner</b>   | The name of the person who is to be sent e-mail or pager alerts regarding events for this group.                      |
| <b>E-mail</b>  | One or more e-mail addresses for the person who is to be sent e-mail or pager alerts regarding events for this group. |
| <b>Members</b> | The objects that are members of the group, sorted by object type.   |

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.

- You can click the column display icon  located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Configuring your dataset for disaster recovery protection

---

Configure your dataset for disaster recovery protection by assigning a disaster recovery policy to it. In this example, to meet data replication requirements, you decide to mirror the primary data to the disaster recovery node and then back up the data to a tertiary node.

## Before you begin

Before beginning this procedure, you need to install the SnapMirror license on all storage systems in the primary and secondary storage nodes.

## About this task

This procedure assumes that you are protecting a new dataset, but you can start at step two if your dataset set is already protected with a backup policy and you want to change the policy to one that is disaster recovery capable.

## Steps

1. Create a disaster recovery capable dataset using the **Add Dataset** wizard.

The wizard prompts you to create a primary node and provision it.

2. In the **Datasets** window, select the dataset and click **Protection Policy** to start the **Dataset Policy Change** wizard.
3. Complete the steps in the wizard to assign the **DR mirror, then backup** policy to the dataset.

The dataset can support failover, and the **Protection Dashboards** window displays failover readiness and failover status panels. The green banners indicate normal states for both.



# Standard protection or disaster recovery protection of datasets

---

Configuration of datasets for disaster recovery protection is similar to configuration of datasets for standard data protection. However, the features provided by disaster recovery protection require some additional dataset configurations.

## Provisioning policies assigned to secondary storage

If you have Provisioning Manager installed and you want to assign an optional provisioning policy to your secondary node. You have the following options:

- In datasets with disaster recovery protection, you can assign either a NAS, SAN, or Secondary storage type provisioning policy to the secondary storage disaster recovery node.
- In datasets with standard protection, you can only assign a Secondary storage type provisioning policy to the secondary node.

**Note:** In all cases, you can chose not to assign a storage policy and assign physical resources directly to each node as was necessary in previous versions of the licensed protection application.

## Exporting data to secondary storage

If you are configuring disaster recovery protection, you have the option to assign an export protocol to the disaster recovery node so that in case of failover, users can access data in the disaster recovery node using the same protocols they used to access data in the original primary node.

- If you have Provisioning Manager installed and you assign a provisioning policy for NAS or SAN type storage to the disaster recovery node, you can also enable export protocols to access that data: CIFS and NFS for NAS type storage; iSCSI and FibreChannel protocol for SAN type storage. Provisioning Manager also exports secondary storage through a vFiler unit if a disaster recovery node is associated with a vFiler unit.
- If you are only configuring standard protection, not disaster recovery protection, you cannot enable export protocols on the secondary storage node through this management application.

## SnapVault and SnapMirror backup protection requirements

- In datasets configured for disaster recovery backup protection, SnapMirror licenses on the primary and disaster recovery node systems are required to support the backup operation. The protection application will configure underlying Qtree SnapMirror relationships that support backup and failover processes between the primary and disaster recovery nodes.
- In datasets configured for standard backup protection, either SnapVault or SnapMirror licenses on the primary and secondary storage systems will support the backup operation.

## Changes in the user interface

Several modifications have been made to the Protection Manager user interface to differentiate datasets configured for standard protection and disaster recovery protection.

### Updated policy graph

The policy graph for a protection policy that is capable of disaster recovery looks similar to a policy graph for a regular protection policy, except that the disaster recovery node is designated with a disaster recovery flag ( ) to indicate the ability of that node to take over primary data node functions if failover is invoked.

### New dashboard windows

The Protection Manager dashboard reports on disaster recovery state and status to provide information at-a-glance that all is well or that something needs attention. In this illustration, the **Failover Readiness** panel and **Failover Status** panel use color, icons, and text to display the state and status for data sets that are capable of disaster recovery. The colors and text vary according to the status of the activity.

Policy wizards, Disaster Recovery tab, and the Policy Overview tab have tables that include a disaster recovery column to indicate whether a policy supports disaster recovery.

The disaster recovery policy and uses a policy icon ( ) to indicate that, if applied, it will protect the data set for disaster recovery.

## **What is the difference between a backup and a disaster recovery backup relationship?**

---

The main difference between protection policies with "Backup" and "DR Backup" (disaster recovery backup) in their labels is that disaster recovery backup protection enables you to perform failover and fallback operations.

However, to ensure the ability to perform such operations, disaster recovery backup protection is subject to limitations placed on its underlying transfer protocol.

- Disaster recovery backup protection always requires underlying qtree SnapMirror (QSM) relationships between containers in the primary node and containers in the secondary disaster recovery node. SnapVault relationships are not supported.
- All relationships created under disaster recovery backup protection are at the Qtree level.
- You cannot add Open Systems SnapVault clients to datasets configured for disaster recovery backup protection.
- Aggregates, volumes, or qtrees that are members of a dataset configured for disaster recovery protection cannot also be members of other datasets.



## What happens during failover

---

When you start the failover process, the licensed application breaks the SnapMirror relationship between the source storage containers in the primary data node and their destination storage containers in the disaster recovery node and activates the disaster recovery node containers as the active systems that can be accessed by users.

When you invoke failover, the licensed protection application puts the dataset into "failing over" state and carries out the following processes.

1. Runs a failover script (if one is specified by the protection policy) to stop applications writing data to the primary storage systems.
2. Quiesces all SnapMirror related activity between the primary storage systems and their partners in the disaster recovery node.
3. Breaks all SnapMirror relationships between the primary storage systems and their partners in the disaster recovery node.
4. Puts any mirrored LUNs in the online state.
5. Runs a failover script (if one is specified by the protection policy) to restart applications writing data to the secondary systems in the disaster recovery node.
6. Enables the same export protocols (CIFS, NFS, iSCSI, or FCP) for the containers in the disaster recovery node as were enabled for the containers in the primary storage systems.
7. After the above processes are complete, the licensed protection application changes the dataset out of failing over state.

If the above processes complete successfully, the dataset state is changed to "failed over." You can now direct or re-map users to access their data from storage in the disaster recovery node.

If one of the above processes failed, the state is changed to "failover error."



# Disaster management options

---

If disaster or mishap jeopardizes the operation of your disaster recovery-capable primary node storage systems, you can use status and event information to assess your backup, failover, or restoration options.

## Events

Path: **Dashboards > Protection > Top Five Events** or **Notifications > Events**

Look for: Hosts down or Volume offline events, which indicate conditions in primary storage that might require failover to storage systems in the disaster recovery node.

## Storage systems status

Path: **Hosts > Storage Systems**

Look for: Storage systems whose System Status column indicates that they are down and might require failover to storage systems in the disaster recovery node. Use the System Status column  button to filter for Down status.

## Disaster recovery failover status

Path: **Data > Datasets > Disaster Recovery**

Look for: The Failover Ready status in the Failover column of the listed disaster recovery capable datasets.

## Disaster recovery failover lag status

Path: **Data > Datasets > Disaster Recovery**

Look for: In Failover Lag status column, whether the last successful backup of primary node data to the disaster recovery node in the listed datasets is satisfactorily current enough for you to invoke failover without a final update.

## Failover readiness

Path: **Dashboards > Protection > Failover Readiness**

Look for: Normal status, which indicates that all disaster recovery capable datasets are ready to undergo failover if necessary.

A Warning or Error status indicates that conditions exist in one or more of your disaster recovery capable datasets that jeopardize successful failover.

## Disaster recovery job progress

Path: **Data > Datasets > Disaster Recovery > Jobs**

Look for: Among other information, the last successful backup or mirror operation (including time started) in a dataset.



# Recovery from disaster

---

In the aftermath of a disaster and successful failover, you can assess whether you need to restore primary storage functions to the storage elements on the original primary node and if so, whether those storage elements need data updated from the current functioning primary storage systems.

Possible recovery actions after failover include the following:

- Make the successful failover target node into the new permanent primary storage system  
Maintain the temporary primary storage systems in the disaster recovery node as the permanent primary storage systems.
- Reactivate the original primary node without updating  
Reactivate and resume forward mirroring from the original primary node without updating its original data.
- Resynchronize to undamaged storage in original primary node  
Resynchronize data from the disaster recovery node to the undamaged storage in the original primary node.
- Resynchronize to destroyed and replaced storage in original primary node  
Resynchronize data from the disaster recovery node to the destroyed and replaced storage in the original primary node.

## Next topics

[\*Making the disaster recovery node the new primary data storage\*](#) on page 649

[\*Recovering by resuming forward mirroring\*](#) on page 651

[\*Recovering by resynchronizing data to undestroyed containers\*](#) on page 652

[\*Recovering by resynchronizing data to replaced containers\*](#) on page 654

## Related tasks

[\*Monitoring failover status\*](#) on page 648



# Fallback options

---

After successful failover, one of your disaster recovery options is to fail back, updating and restoring primary storage function to the original primary storage node, either to undestroyed volumes and qtrees, or to replaced volumes and qtrees.

- If you want to fail back to volumes or qtrees that remain undestroyed in the original primary data node, follow the instructions in the help topic titled "Recovery by resynchronizing data to undestroyed containers" in the disaster recovery help.
- If you want to fail back to replaced volumes or qtrees in the original primary data node, follow the instructions in the help topic titled "Recovery by resynchronizing data to replaced containers" in the disaster recovery help.

## Related tasks

[\*Recovering by resynchronizing data to undestroyed containers\*](#) on page 652

[\*Recovering by resynchronizing data to replaced containers\*](#) on page 654



# How do I back up data?

---

You can back up data from an entire host, or from individual aggregates, volumes, qtrees, virtual machines, or directories on the host.

## About this task

Complete the following steps to back up data. Following each step is one or more online help topics that describe how to perform the step. For links to each online help topic, see the related links below. For an example workflow of setting up data protection in Protection Manager, see the *Provisioning Manager and Protection Manager Administration Guide*.

## Steps

1. Add the host.
  - How hosts become visible to the console
  - Adding a storage system
  - Adding an Open Systems SnapVault (OSSV) host
  - Guidelines for adding and editing an Open Systems SnapVault host on an ESX 3.5 server
2. Configure a resource pool.
  - Adding a resource pool
3. Choose a protection policy.
  - Adding a protection policy
4. Create additional schedules as needed.
  - Decisions to make before adding a schedule
5. Assign the schedules to the protection policy.
  - Assigning or changing schedules in a protection policy
6. Create one or more groups.
  - Adding groups
7. Create a dataset.
  - Adding a dataset
8. Attach the protection policy to the dataset.
  - Applying or changing the protection policy to a dataset

**9.** Verify the protection of the dataset.

- Where to find logs

**10.** Configure alarms.

- Adding alarms

**Related concepts**

*How hosts become visible to the console* on page 901

*Decisions to make before adding a protection policy* on page 251

*Where to view reports and logs* on page 977

**Related tasks**

*Adding a storage system* on page 915

*Adding an Open Systems SnapVault host* on page 921

*Adding a resource pool* on page 841

*Assigning or changing schedules in a protection policy* on page 325

*Adding groups* on page 461

*Adding a dataset* on page 719

*Assigning or changing a protection policy* on page 725

*Adding alarms* on page 601

**Related references**

*Guidelines for adding and editing an Open Systems SnapVault host on an ESX server* on page 919

**Related information**

*Provisioning Manager and Protection Manager Administration Guide -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)*

## Protect Now details

---

Where appropriate, Protection Manager will retain the backup copies according to the assigned protection policy's settings for the retention type (Hourly, Daily, Weekly, Monthly, or "Retain until deleted manually") that you select.

**Note:** In some cases, the mode of back up or an application-defined retention schedule renders the retention type that you specify here inapplicable.

If you have applied a throttle schedule to the dataset, that schedule will also apply to the on-demand back up.



# How the protection application supports deduplication

---

Deduplication is the consolidation of blocks of duplicate data into single blocks to store more information using less storage space. The protection application supports protection of volumes on which deduplication is enabled; however, you can not enable or manage deduplication through NetApp Management Console unless you license the provisioning application.

- If the provisioning application is licensed, you can configure your provisioning policies to enable deduplication in on-demand, automated, scheduled mode for your protected volumes and dataset nodes.
- If the provisioning application is not licensed, you can still enable, manage, and monitor deduplication on individual storage systems using the Data ONTAP CLI.  
Protection operations started from the protection application will not affect the deduplication processes invoked through Data ONTAP CLI if the provisioning application is not licensed.
- If the provisioning application is licensed after deduplication has been configured through the Data ONTAP CLI, be sure to enable the deduplication option in the provisioning policy that you assign to your dataset node.  
If you do not, the provisioning policy overrides the storage system configuration and the deduplication capability is discontinued.

For more information on CLI implementation of deduplication see *Data ONTAP Data Protection Online Backup and Recovery Guide*.

## Related concepts

[What deduplication is](#) on page 799

## Related information

*Data ONTAP Data Protection Online Backup and Recovery Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)



## **"Warn about overwrite and out-of-space conditions on the destination" option**

---

The "Warn about overwrite and out-of-space conditions on the destination" option configures the **Restore** wizard to warn about file overwrite or out-of-space conditions during a file-level restore from a storage system backup.

**Note:** This option enables warnings only for file-level restores from storage system backups. **Restore** wizard does not issue warnings for volume-level restores, qtree-level restores, folder-level restores, restores from Open Systems SnapVault backups, or restores from ESX server backups.



# What vFiler templates are

---

A vFiler template is a set of vFiler configuration settings, including the corresponding CIFS, DNS, NIS, and administrative host configuration settings, that you want to use as default settings for one or more vFiler units that you plan to add as hosts. You can configure as many vFiler templates as you need.

When adding a vFiler unit as a host, you can specify a vFiler template that provides the default configuration settings for that vFiler unit. In addition to the configuration settings provided by the vFiler template, you also must specify those values that are unique to the vFiler unit, such as name and IP address.

## Related concepts

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

[\*Decisions to make before adding vFiler templates\*](#) on page 891



# What a policy is

---

A policy is a set of rules that specifies the intended management of dataset members. You can apply the same policy to multiple datasets, leveraging your configuration of the policy across the datasets. If you update a policy, the update is propagated across all the datasets to which the policy is applied. Different types of policies address different data management issues.

Depending on the licenses you have installed, the data management applications provide the following types of policies:

- Protection without disaster recovery
- Protection with disaster recovery
- Provisioning
- vFiler templates

**Note:** The data management policies used by applications running in NetApp Management Console should not be confused with other kinds of policies, such as the file policies used in Data ONTAP.

## Next topics

- [\*What a protection policy is\*](#) on page 847
- [\*What a provisioning policy is\*](#) on page 848

## Related concepts

- [\*Dataset concepts\*](#) on page 693



# Adding alarms

---

You can add an alarm when you want immediate notification that a specified event or event class or event of a specified severity level occurred.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available to complete this task:

- The resource group with which you want the alarm associated.
- The event name, event class, or severity type that triggers the alarm.
- Who and what you want the event notification sent to.
- The time period during which the alarm is active.
- Whether you want the event notification repeated until the event is acknowledged and how often the notification should be repeated.

## Steps

1. For licensed applications, from the navigation pane, click **Notifications > Alarms**. For Performance Advisor, from the navigation pane, click the **Set Up Alarms** window.
2. Click **Add** to start the **Add Alarm** wizard.
3. On each page of the wizard, enter the appropriate information.
4. Click **Finish** to commit your choices and close the **Add Alarm** wizard.
5. Verify the creation and configuration of the alarm by viewing the results that are displayed in the **Alarms** window.

## After you finish

You can edit the alarm properties from the **Alarms** window.

## Related concepts

[Decisions to make before adding an alarm](#) on page 83

[How to know when an event occurs](#) on page 41

## Related tasks

[How do I back up data?](#) on page 589

## Related references

[Alarm properties](#) on page 79

*Administrator roles and capabilities* on page 1055

# Administrator roles and capabilities

---

The administrator roles determine the tasks you can perform using applications in NetApp Management Console .

## Default and custom roles

One or more capabilities must be specified for every role, and you can assign multiple capabilities if you want the administrator to have more control than a specific role provides. For example, if you want an administrator to perform both the backup and restore operations, you must assign Back Up and Restore roles to the administrator.

The DataFabric Manager server and the client applications provide a set of default global roles described in the following list. You can customize these roles and the capabilities associated with them and you can create new ones using the Operations Manager Web-based user interface. For more information about configuring role-based access control (RBAC), see the *Operations Manager Administration Guide* .

<b>GlobalBackup</b>	You can initiate a backup to any secondary volume and ignore discovered hosts.
<b>GlobalDataProtection</b>	You can initiate a backup to any secondary volume; view backup configurations, events and alerts, and replication or failover policies; and import relationships into datasets.
<b>GlobalDataset</b>	You can create, modify, and delete datasets.
<b>GlobalDelete</b>	You can delete information in the DataFabric Manager server database, including groups and members of a group, monitored objects, custom views, primary and secondary storage systems, and backup relationships, schedules, and retention policies.
<b>GlobalEvent</b>	You can view, acknowledge, and delete events and alerts.
<b>GlobalFullControl</b>	You can view and perform any operation on any object in the DataFabric Manager server database and configure administrator accounts. You cannot apply this role to accounts with group access control.
<b>GlobalMirror</b>	You can create, destroy, and can update replication or failover policies.
<b>GlobalRead</b>	You can view the DataFabric Manager server database, backup and provisioning configurations, events and alerts, performance data, and policies.
<b>GlobalRestore</b>	You can restore the primary data back to a point in time or restore to a new location.
<b>GlobalWrite</b>	You can view or write to the DataFabric Manager server database.

<b>GlobalResourceControl</b>	You can add members to dataset nodes that are configured with provisioning policies.
<b>GlobalProvisioning</b>	You can provision primary dataset nodes and can attach resource pools to secondary or tertiary dataset nodes. The GlobalProvisioning role also includes all the capabilities of the GlobalResourceControl, GlobalRead, and GlobalDataset roles for dataset nodes that are configured with provisioning policies.
<b>GlobalPerfManagement</b>	You can manage views, event thresholds, and alarms apart from viewing performance information in Performance Advisor.

### Related concepts

[\*Strategies for enabling a dataset for migration\*](#) on page 779

### Related tasks

[\*Printing Help topics\*](#) on page 111

[\*Adding alarms\*](#) on page 601

[\*Testing alarms\*](#) on page 87

[\*Editing alarms\*](#) on page 89

[\*Deleting alarms\*](#) on page 91

[\*Responding to alarms\*](#) on page 95

[\*Monitoring alarms\*](#) on page 97

[\*Enabling and disabling alarms\*](#) on page 99

[\*Monitoring events\*](#) on page 65

[\*Responding to and acknowledging events\*](#) on page 67

[\*Deleting events\*](#) on page 69

[\*Adding a dataset\*](#) on page 719

[\*Assigning or changing a protection policy\*](#) on page 725

[\*Provisioning resources for a primary dataset node\*](#) on page 731

[\*Changing dataset node resource assignments\*](#) on page 739

[\*Adding resources to a dataset\*](#) on page 737

[\*Changing dataset node resource assignments\*](#) on page 739

[\*Removing resources from a dataset\*](#) on page 741

[\*Editing dataset general properties\*](#) on page 753

[\*Deleting a dataset\*](#) on page 755

[\*Adding a resource pool\*](#) on page 841

[\*Editing resource pool properties\*](#) on page 845

[\*Adding groups\*](#) on page 461

[\*Editing groups\*](#) on page 463

*Deleting groups* on page 465  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943  
*Updating Open Systems SnapVault client data* on page 945  
*Diagnosing a storage system* on page 947  
*Diagnosing an Open Systems SnapVault host* on page 949  
*Adding a daily protection schedule* on page 307  
*Adding a weekly protection schedule* on page 309  
*Adding a monthly protection schedule* on page 311  
*Adding a throttle schedule* on page 313  
*Deleting a protection or throttle schedule* on page 323  
*Assigning or changing schedules in a protection policy* on page 325  
*Copying a protection or throttle schedule* on page 327  
*Monitoring dataset status* on page 403  
*Monitoring backup and mirror relationships* on page 405  
*Backing up datasets on-demand* on page 407  
*Suspending protection of datasets* on page 409  
*Suspending data protection for backup volume maintenance* on page 411  
*Resuming protection of datasets* on page 413  
*Restoring backed-up data to a new location* on page 423  
*Restoring backed-up data over current data* on page 425  
*Restoring selected portions of a dataset* on page 427  
*Restoring a virtual machine to its original location* on page 429  
*Restoring a virtual machine file system to any location* on page 431  
*Restoring a virtual machine to its original location through another ESX server* on page 433  
*Importing discovered external relationships* on page 451  
*Adding unprotected host data to an existing dataset* on page 443  
*Adding unprotected host data to a new dataset* on page 445  
*Protecting unprotected datasets* on page 447  
*Starting a vFiler unit migration* on page 961  
*Updating vFiler unit migration SnapMirror relationships* on page 963  
*Cutting over to the new vFiler unit destination* on page 965  
*Cleaning up a vFiler unit migration* on page 967

- Cancelling a vFiler unit migration* on page 969
- Viewing vFiler unit migration status* on page 971
- Adding a protection policy* on page 671
- Editing a policy's primary data node* on page 258
- Editing a policy's backup connection* on page 259
- Editing a policy's backup node* on page 260
- Editing a policy's mirror connection* on page 260
- Editing a policy's mirror node* on page 261
- Changing retention times in a protection policy* on page 265
- Changing lag thresholds in a protection policy* on page 267
- Changing a node name in a policy* on page 269
- Deleting a protection policy* on page 271
- Editing a daily schedule* on page 315
- Editing a weekly schedule* on page 317
- Editing a monthly schedule* on page 319
- Editing a throttle schedule* on page 321
- Assigning or changing a provisioning policy* on page 727
- Configuring dataset nodes for NFS protocol access* on page 747
- Configuring dataset nodes for CIFS protocol access* on page 745
- Configuring dataset nodes for FC protocol access* on page 749
- Configuring dataset nodes for iSCSI protocol access* on page 751
- Displaying export properties for a specific dataset member* on page 417
- Displaying export and mapping information for all members of a dataset node* on page 415
- Monitoring failover readiness* on page 643
- Testing failover scripts* on page 644
- Updating disaster recovery node storage before failover* on page 646
- Starting failover* on page 647
- Monitoring failover status* on page 648
- Making the disaster recovery node the new primary data storage* on page 649
- Recovering by resuming forward mirroring* on page 651
- Recovering by resynchronizing data to undestroyed containers* on page 652
- Recovering by resynchronizing data to replaced containers* on page 654
- Testing failover scripts* on page 644
- Enabling disaster recovery protection* on page 641
- Adding a dataset* on page 719
  - Configuring dataset nodes for CIFS protocol access* on page 745
  - Configuring dataset nodes for NFS protocol access* on page 747
  - Configuring dataset nodes for iSCSI protocol access* on page 751
  - Configuring dataset nodes for FC protocol access* on page 749

*Assigning or changing a protection policy* on page 725  
*Provisioning resources for a primary dataset node* on page 731  
*Changing dataset node resource assignments* on page 739  
*Adding resources to a dataset* on page 737  
*Removing resources from a dataset* on page 741  
*Editing dataset general properties* on page 753  
*Deleting a dataset* on page 755  
*Viewing volume, LUN or qtree space allocation* on page 757  
*Diagnosing volume or qtree space status* on page 759  
*Diagnosing volume or qtree space status* on page 759  
*Resizing volume space* on page 761  
*Resizing qtree space* on page 763  
*Deleting Snapshot copies* on page 765  
*Deleting a volume, LUN or qtree* on page 767  
*Enabling deduplication on your dataset nodes* on page 809  
*Disabling deduplication on dataset nodes* on page 811  
*Starting on-demand deduplication* on page 813  
*Stopping an in-progress deduplication* on page 815  
*Viewing volume-level deduplication space-saving* on page 817  
*Adding a resource pool* on page 841  
*Editing resource pool properties* on page 845  
*Viewing a provisioning policy* on page 859  
*Adding a provisioning policy* on page 875  
*Editing a provisioning policy* on page 879  
*Copying a provisioning policy* on page 881  
*Deleting a provisioning policy* on page 883  
*Viewing vFiler templates* on page 889  
*Adding a vFiler template* on page 893  
*Editing a vFiler template* on page 895  
*Copying a vFiler template* on page 897  
*Deleting a vFiler template* on page 899  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943

- Updating Open Systems SnapVault client data* on page 945
- Diagnosing a storage system* on page 947
- Diagnosing an Open Systems SnapVault host* on page 949
- Monitoring jobs* on page 973
- Cancelling jobs* on page 975
- Starting a dataset migration* on page 783
- Updating dataset migration SnapMirror relationships* on page 785
- Cutting over to the new dataset storage destination* on page 787
- Cleaning up a dataset migration* on page 789
- Relinquishing migration capability of a dataset* on page 797
- Cancelling a dataset migration* on page 791
- Viewing dataset migration status* on page 793
- Assigning or changing a provisioning policy* on page 727

#### **Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Disaster recovery capable protection policies

---

Disaster recovery capable protection policies are data protection policies that support supplemental primary-to-disaster recovery node failover instructions, which you can invoke if the primary node is disabled or destroyed. Failover quickly transfers primary node functions and availability to your disaster recovery node, allowing your users to continue to access and input data as if the original primary node were still operating.

The licensed protection application provides policy templates for you to use to configure the following types of backup setups.

<b>DR Back up</b>	A dataset is backed up from primary storage to secondary storage on a disaster recovery node. If disaster or mishap disables or destroys primary storage, secondary storage takes over and provides primary storage availability.
<b>DR Back up, then mirror</b>	A dataset is backed up from primary storage to secondary storage on a disaster recovery node and from there mirrored to a tertiary node. If disaster or mishap disables or destroys primary storage, secondary storage is enabled to take over and provide primary storage function and availability.
<b>DR Mirror, then mirror</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node and from there mirrored again to a tertiary node. If disaster or mishap disables or destroys primary storage, the mirrored storage on the disaster recovery node is enabled to take over and provide primary storage function and availability.
<b>DR Mirror</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node. If disaster or mishap disables or destroys primary storage, the mirrored storage on the disaster recovery node is enabled to take over and provide primary storage function and availability.
<b>DR Mirror and back up</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node and is also backed up to secondary storage on a SnapVault or SnapMirror storage system . If mishap or disaster disables or destroys primary storage, the secondary storage on the disaster recovery node takes over and provides primary storage availability.
<b>DR Mirror and mirror</b>	A dataset is mirrored from primary storage to secondary storage on two different SnapMirror partners. If mishap or disaster disables or destroys primary storage, the SnapMirror partner in the disaster recovery node takes over and provides primary storage function and availability.
<b>DR Mirror, then back up</b>	A dataset is mirrored from primary storage to secondary storage on the destination recovery node and from there backed up to tertiary storage on a SnapVault or SnapMirror storage system . If mishap or disaster disables or

destroys primary storage, the secondary storage in the destination recovery node takes over and provides primary storage function and availability.

**Related references**

*[Protection policies \(not disaster recovery capable\)](#)* on page 669

# Recovering by resynchronizing data to undestroyed containers

---

After a successful failover, you can use the `dfpm` and `dfdrm` commands on the DataFabric Manager server to restore primary storage function to your original undestroyed primary storage systems and containers and update their data with the most recent changes made to their failover partners in the disaster recovery node.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. Log in to the DataFabric Manager server to which your licensed protection application is assigned.
2. In the command line interface, enter the command:

```
dfpm dataset list -R data_set_name
```

This step finds the secondary storage elements for all primary storage elements. SnapMirror relationships that were broken during the failover are indicated by the "broken\_off" state.

3. If your protection policy is based on the DR Mirror and Mirror node mapping, enter the command:

```
dfdrm mirror break non_dr_obj1 non_dr_obj2 non_dr_obj3 non_dr_obj...
```

This command breaks the SnapMirror relationships between source volumes and qtrees in the primary node and destination volumes and qtrees in the non-disaster recovery node.

Skip to Step 5.

4. If your protection policy is based on the DR Mirror then Mirror node mapping, enter the command:

```
dfdrm mirror break tertiary_obj1 tertiary_obj2 tertiary_obj3 tertiary_obj...
```

This command breaks the SnapMirror relationships between source volumes and qtrees in the disaster recovery node and destination volumes and qtrees in the tertiary node.

5. Enter the command:

```
dfdrm mirror resync -r dr_obj1 dr_obj2 dr_obj3 dr_obj...
```

This command temporarily reverses the original SnapMirror relationships (which updates the original primary storage containers as SnapMirror destinations).

In this command, *dr\_obj...* is all volumes and qtrees in the disaster recovery node, now serving as primary storage, that you want to temporarily configure as a SnapMirror sources.

Wait for all relationships to be in the "snapmirrored" state before continuing to the next Step.

**6.** Enter the command:

```
dfdrm mirror break original_obj1 original_obj2 original_obj3 original_obj...
```

This command quiesces and breaks the temporary reversed mirror relationships.

In this command, *original\_obj...* is all original primary objects that are temporarily configured as SnapMirror destinations.

**7.** After you break the reversed mirror relationship, inspect the data on the original primary objects to verify validity.

**8.** Enter the command:

```
dfdrm mirror resync -r original_obj1 original_obj2 original_obj3 original_obj...
```

This command resyncs the mirror copies to reestablish the original SnapMirror relationships (in other words, to reverse the relationships back to forward mirror).

**9.** If your protection policy is based on the DR Mirror and Mirror node mapping, enter the command:

```
dfdrm mirror resync non_dr_obj1 non_dr_obj2 non_dr_obj3 non_dr_obj...
```

This command resyncs the mirror copies to reestablish the original primary node to non-disaster recovery secondary node SnapMirror relationships.

Skip to Step 11.

**10.** If your protection policy is based on the DR Mirror then Mirror node mapping, enter the command:

```
dfdrm mirror resync tertiary_obj1 tertiary_obj2 tertiary_obj3 tertiary_obj...
```

This command resyncs the mirror copies to reestablish the original disaster recovery node to tertiary node SnapMirror relationships.

**11.** Confirm the success of the resync operation by noting its job list ID output and entering the command:

```
dfdrm job list joblist_id
```

If the job list command indicates a resync job failure, then reinitialize the mirror relationship between each volume or qtree by using the command

```
dfdrm mirror initialize dr_obj tertiary_obj
```

**12.** Enter the command:

```
dfpm dataset failover state dataset-name ready
```

This command sets the dataset disaster recovery state to ready.

**Related concepts**

*[Fallback options](#)* on page 587

**Related references**

*[Administrator roles and capabilities](#)* on page 1055



# Recovering by resynchronizing data to replaced containers

---

After a successful failover, you can use the `dfpm` and `dfdrm` commands on the DataFabric Manager server to restore primary storage function to destroyed and replaced original primary storage containers and resynchronize primary storage data with the most recent updates.

## Before you begin

- At the original primary storage site, confirm that the destroyed storage systems, aggregates, volumes, and qtrees are replaced with containers of the same name, capacity, and configuration.  
**Note:** Configure the replacement volumes in restricted (not online or offline) state.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

- Log in to the DataFabric Manager server to which your licensed protection application is assigned.
- In the command line interface, enter the command:

```
dfpm dataset list -R data_set_name
```

This step finds the secondary storage elements for all primary storage elements. SnapMirror relationships that were broken during the failover are indicated by the "broken\_off" state.

- Enter the command:

```
dfpm dataset list -m -M data_set_name
```

This step lists the missing (destroyed) containers in the specified dataset.

- After listing the missing containers, in each system with a missing container, use FilerView or the Data ONTAP CLI to recreate the missing aggregates, volumes, or qtrees. Configure the replacement volumes with restricted (not online or offline) state.
- If your disaster recovery protection policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror delete non_dr_obj1
```

This step deletes the non-disaster recovery node mirror destination objects.

- Enter the command:

```
dfdrm mirror initialize dr_obj_name1 replaced_obj_name
```

This command creates a new SnapMirror relationship to the replacement volumes and qtrees in the original primary node from their source partner volumes and qtrees in the disaster recovery node. It temporarily configures the disaster recovery node volumes and qtrees as SnapMirror source objects and the replacement volumes and qtrees as destination objects. It then copies the updated data from the volumes and qtrees in the disaster recovery node to the replacement volumes and qtrees in the original primary node.

**Note:** Because you cannot create a SnapMirror relationship to a replacement aggregate, use this command to create SnapMirror relationships to that aggregate's child volumes instead.

7. Repeat Step 6 for each disaster recovery node volume or qtree that has a replacement volume or qtree.
8. After the mirror initialize operations are complete, enter the command:

```
dfdrm mirror quiesce replaced_obj1 replaced_obj2 replaced_obj3  
replaced_obj...
```

This step quiesces these new mirror relationships prior to breaking and reversing them. In this command, *replaced\_obj...* is all the replacement containers that you have just updated.

9. Enter the command:

```
dfdrm mirror break replaced_obj1 replaced_obj2 replaced_obj3 replaced_obj...
```

This command breaks the current mirror relationships prior to reversing them.

10. After you break the mirror relationship, inspect the data on the original primary objects to verify validity.

11. Enter the command:

```
dfdrm mirror resync -r replaced_obj1replaced_obj2  
replaced_obj3replaced_obj...  
to reverse the mirror relationship.
```

This action establishes the replacement volumes and qtrees as the primary storage containers and the volumes and qtrees in the disaster recovery node as the SnapMirror destination objects.

12. If your disaster recovery protection policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror initialize replaced_obj...non_dr_obj...
```

This command creates a new SnapMirror relationship between the replacement volumes and qtrees in the original primary node and their partner volumes and qtrees in the non-disaster recovery node. It temporarily configures the disaster recovery node volumes and qtrees as SnapMirror source objects and the replacement volumes and qtrees as destination objects.

Repeat this command for each replaced volume or qtree in the primary node.

13. If your disaster recovery policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror resyncnon_dr_obj1non_dr_obj2non_dr_obj..non_dr_obj3
```

This command updates the empty volumes and qtrees in the non-disaster recovery node with data from their replaced partners in the primary node. In this command, *non\_dx\_obj...* is all the volumes and qtrees in the non-disaster recovery node that you want to update.

Wait for all relationships to be in the "snapmirrored" state.

**14.** Enter the command:

```
dfpm dataset replace dataset-name
```

This command replaces the dataset reference to old primary volumes and qtrees with replaced volumes and qtrees.

**Note:** This step carries out replacement of old with new volume and qtree references only. To replace old with new aggregate references in the failed back dataset, see the next step.

**15.** If the failed-back dataset originally included aggregates, complete the following commands to add reference to the replacement aggregates and delete reference to their child volumes in the failed-back dataset.

Even though the failed aggregate was destroyed and replaced, you still need to complete the following steps to reference the replacement aggregate in the failed-back dataset.

**a.** Enter the command:

```
dfpm dataset list -m dataset_name
```

This command lists the child members (volumes or qtrees) of the replacement aggregate.

**b.** Enter the command:

```
dfpm dataset remove dataset_name child_obj
```

.

This command removes reference to the child members of the replacement aggregates from this dataset.

Even though references to the child replacement volumes are removed from the dataset, the SnapMirror relationships and operations between these replacement volumes and their disaster recovery node mirrors remain intact.

**c.** Enter the command:

```
dfm aggr list storage_system
```

This command lists the replacement aggregate at the primary site.

**d.** Enter the command:

```
dfpm dataset add dataset_name replacement_aggr
```

This command adds the replacement aggregate to the failed back dataset.

**e.** Enter the command:

```
dfpm dataset list -m dataset_name
```

This command confirms the addition of the replacement aggregate to this dataset by listing the dataset contents.

- 16.** Enter the command:

```
dfpm dataset list -R dataset_name
```

This step confirms the disaster recovery relationship between the replacement child volumes and their destinations in the disaster recovery node.

- 17.** Enter the command:

```
dfpm dataset failover state dataset_name ready
```

This step sets the dataset disaster recovery state to ready.

#### Related concepts

[\*Fallback options\*](#) on page 587

#### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# What deduplication is

---

Deduplication is a provisioning application option that you can enable on your storage nodes to eliminate duplicate data blocks to reduce the amount of storage space used to store active data.

On the affected volumes, deduplication allows you to reduce the amount of space used to store active data, or even allows you to purposely over deduplicate and store more bytes of data than the capacity of the available physical storage.

You can enable your provisioning policies to support three modes of deduplication.

<b>On-demand deduplication</b>	On-demand deduplication is executed on a selected volume that is enabled for deduplication when you click the <b>Dedupe Now</b> button on your Provisioning tab.
<b>Automated</b>	Automated deduplication, if enabled on a dataset node, is run automatically on any volume in that node when the amount of new data written to that volume reaches 20%.
<b>Scheduled deduplication</b>	Scheduled deduplication, if enabled on a dataset node, is run automatically on the volumes in that node on the days of the week, during a particular time period, and at a frequency that you have specified.

## Related concepts

[How the protection application supports deduplication](#) on page 593



# Relinquishing migration capability of a dataset

---

You can relinquish the migration capability of a dataset by removing the vFiler unit assignment for the dataset.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

When provisioning a dataset, or starting a dataset migration, you might encounter a message that the maximum number of vFiler units has been reached. When this occurs, you might need to relinquish the migration capability of one or more datasets.

**Note:** This operation destroys the attached vFiler unit and relinquishes the contained resources (for example, the volumes, the qtrees, the quotas, and the NFS, CIFS, and iSCSI exports to the hosting storage system).

## Steps

- From the navigation pane, click **Data > Datasets > Migration**.

You can also relinquish the migration capability of a dataset in the **Edit Dataset** window.

- Select a dataset that has a vFiler unit assigned and for which you want to remove the migration capability, and click **Relinquish migration capability**.

The "Relinquish migration capability" button is enabled only for datasets that have an attached vFiler unit that was created when the dataset was first added.

The provisioning application performs a test of the modification and lists all resulting errors and warnings in the **Preview Details** window.

- In the confirmation dialog box, click **Relinquish**.

## Related concepts

[When to relinquish the migration capability of a dataset](#) on page 777

## Related tasks

[Adding a dataset](#) on page 719

## Related references

[Administrator roles and capabilities](#) on page 1055



# What disaster recovery protection is

---

The disaster recovery feature enhances your data protection services by enabling you to continue to provide data access to your users, even in the event of a mishap or disaster that disables or destroys the storage systems in your primary node.

If disaster recovery protection is installed, you can quickly enable your secondary storage systems to provide primary data storage access to your users with little or no interruption, until your primary storage systems are reenabled or replaced.

To use the disaster recovery feature, you must enable the disaster recovery license on your system. You must also have the protection license enabled.

**Note:** The protection application provides disaster recovery protection of data fronted by vFiler units; however, it does not support disaster recovery protection as implemented by the Data ONTAP vFiler DR feature.

## Next topics

[When you use disaster recovery](#) on page 623

[Recovery strategies after failover](#) on page 624

[Disaster recovery protection tasks](#) on page 624

## When you use disaster recovery

If a mishap or disaster disables or destroys the storage systems at a primary storage site, you can invoke a failover process that breaks the SnapMirror relationship between the primary and secondary partners and transfers primary storage site functions (including continued user access) to the mirror partners at the secondary storage site.

In a typical disaster recovery protection implementation, the storage systems at the primary storage site use underlying SnapMirror processes to maintain recent Snapshot copies and active copies of their data. These copies are located on SnapMirror partners at a secondary site that is located a safe distance from the primary storage site.

With sufficient warning of an impending event that threatens the primary storage site, the administrator can invoke a final Snapshot copy transfer from the primary site to the secondary storage site and can monitor the entire system for failover readiness in case there needs to be failover.

## Recovery strategies after failover

After storage systems at the original primary storage site are reenabled or replaced, you can implement one of the following recovery strategies.

- Resume forward mirroring from the original primary storage site, using the data still available at that site.
- Complete offline restoration of updated data from the failover site to the original primary storage site and then resume forward mirroring.
- Use the command-line interface to fail back primary storage site function from the failover site to the original site, with little off-line time.

## Disaster recovery protection tasks

Disaster recovery protection consists of one or more of the following tasks.

- Configure disaster recovery capable protection policies.
- Author optional failover scripts for managing data application tasks before and after the SnapMirror relationship break.
- Assign disaster recovery capable protection policies to datasets.
- Test disaster recovery capable protection policies.
- Monitor primary and secondary storage for failover readiness.
- Update secondary storage in preparation for failover.
- In case of emergency, assess appropriate disaster recovery protection measures to implement.
- In case of emergency, perform and monitor failover operations.
- If necessary, perform failback recovery operations.

# Disaster recovery concepts

---

It is helpful to have an understanding of the basic disaster recovery concepts.

The implementation of disaster recovery protection in the licensed protection application relies on the following concepts:

<b>Failover</b>	An automated process which, when invoked, transfers primary storage capability and accessibility from threatened, disabled, or destroyed storage systems in a primary node to secondary storage systems in the disaster recovery node.
<b>Failback</b>	Command-line based procedures that restore primary storage function to the original primary storage site after its storage systems are reenabled or replaced.
<b>Disaster recovery capable</b>	Describes a dataset that is configured with the protection policies and provisioned with the primary storage and secondary storage resources to support disaster recovery protection.
<b>Disaster recovery node</b>	The dataset secondary storage node that is configured to also provide failover primary storage access to users in the event of mishap or disaster making the original primary storage systems unavailable.
<b>Disaster recovery relationship</b>	The type of data protection and failover procedures configured between the primary storage and secondary storage systems (in the disaster recovery node), and between the secondary storage systems and any tertiary storage systems.
<b>Qtree SnapMirror</b>	The technology that supports qtree-to-qtree disaster recovery capable backup relationships in the licensed protection application and possible failover operations between primary storage systems and secondary storage systems. In disaster recovery protection policies, secondary storage is located in the disaster recovery node.
<b>Volume SnapMirror</b>	The technology that supports volume-to-volume disaster recovery capable mirror relationships in the licensed application and possible failover operations between primary storage and secondary storage systems. In disaster recovery protection policies, secondary storage is located in the disaster recovery node.
<b>SnapMirror relationship break</b>	The automated event during failover that breaks the SnapMirror relationship between primary storage and secondary storage in the disaster recovery node.
<b>Failover state</b>	Dashboard status in the licensed application that indicates the progress and success of a failover operation if the failover process is invoked. Possible states include: Ready, Failing over, Failed over, and Failover Error.
<b>Failover readiness</b>	Dashboard status in the licensed application that indicates the readiness of the managed datasets to successfully carry out failover operations.

<b>Failover script</b>	An optional user-authored script that specifies data application-related operations that might need to be performed before and after the failover invoked SnapMirror relationship break between primary storage and secondary storage in the disaster recovery node.
<b>Rebaselining</b>	The protection backup or mirroring of data by the transfer or copy of the entire body of data from primary to secondary or secondary to tertiary storage. All initial backup or mirror operations from primary to secondary or secondary to tertiary storage are baseline operations and can be quite lengthy. Succeeding backup or mirror operations can be incremental, involving only the transfer from source to destination that has changed since the last backup or mirror operation. When assigning a new protection policy (disaster recovery capable or not) after a disaster and successful failover, the most preferable choice might be to assign and set up a protection policy that minimizes rebaselining of data in the primary, secondary, and tertiary storage.

## Disaster recovery capable protection policies

---

Disaster recovery capable protection policies are data protection policies that support supplemental primary-to-disaster recovery node failover instructions, which you can invoke if the primary node is disabled or destroyed. Failover quickly transfers primary node functions and availability to your disaster recovery node, allowing your users to continue to access and input data as if the original primary node were still operating.

The licensed protection application provides policy templates for you to use to configure the following types of backup setups.

<b>DR Back up</b>	A dataset is backed up from primary storage to secondary storage on a disaster recovery node. If disaster or mishap disables or destroys primary storage, secondary storage takes over and provides primary storage availability.
<b>DR Back up, then mirror</b>	A dataset is backed up from primary storage to secondary storage on a disaster recovery node and from there mirrored to a tertiary node. If disaster or mishap disables or destroys primary storage, secondary storage is enabled to take over and provide primary storage function and availability.
<b>DR Mirror, then mirror</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node and from there mirrored again to a tertiary node. If disaster or mishap disables or destroys primary storage, the mirrored storage on the disaster recovery node is enabled to take over and provide primary storage function and availability.
<b>DR Mirror</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node. If disaster or mishap disables or destroys primary storage, the mirrored storage on the disaster recovery node is enabled to take over and provide primary storage function and availability.
<b>DR Mirror and back up</b>	A dataset is mirrored from primary storage to secondary storage on the disaster recovery node and is also backed up to secondary storage on a SnapVault or SnapMirror storage system . If mishap or disaster disables or destroys primary storage, the secondary storage on the disaster recovery node takes over and provides primary storage availability.
<b>DR Mirror and mirror</b>	A dataset is mirrored from primary storage to secondary storage on two different SnapMirror partners. If mishap or disaster disables or destroys primary storage, the SnapMirror partner in the disaster recovery node takes over and provides primary storage function and availability.
<b>DR Mirror, then back up</b>	A dataset is mirrored from primary storage to secondary storage on the destination recovery node and from there backed up to tertiary storage on a SnapVault or SnapMirror storage system . If mishap or disaster disables or

destroys primary storage, the secondary storage in the destination recovery node takes over and provides primary storage function and availability.

**Related references**

*[Protection policies \(not disaster recovery capable\)](#)* on page 669

# Protection policy node prerequisites

---

Before you attempt to implement a protection policy on your dataset nodes, ensure that the storage systems in the datasets or physical resource pools that make up that node meet the correct configuration and licensing requirements.

- Storage that is the source of a backup connection (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume, qtree, or OSSV directory if it is not an application dataset
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVault Data ONTAP Primary (for remote backup protection)
- Storage that is the source of a backup connection configured for nondisruptive LUN restore (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume or qtree
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requires both of the following:
    - Data ONTAP Primary
    - Data ONTAP 7.3 or later
- Storage that is the source of a disaster recovery capable backup connection (to a NetApp storage system )
  - Configuration requirements are all of the following:
    - Qtree, volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes)
    - Dataset not configured for non-disruptive LUN restore
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a backup connection (Open System)
  - Configuration requirements: Open Systems SnapVault directory

- Storage system licensing requirements: Open Systems SnapVault client
- Storage that is the destination of a backup connection (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume
    - Qtree
    - Storage system or aggregate containing volumes and qtrees
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVaultData ONTAP Secondary (for remote backup protection)  
If the source is Windows, Linux, or UNIX, then SnapVault Windows, SnapVault Linux, or SnapVault UNIX is also required.
- Storage that is the destination of a backup connection configured for nondisruptive LUN restore (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Qtree or volume
    - Storage system or aggregate containing volumes and qtrees. Provisioning policy type (SAN or NAS) matches primary provisioning policy type or does not export storage.
  - Storage system licensing requirements are all of the following:
    - SnapVault
    - Data ONTAP Secondary
    - Data ONTAP 7.3 or later
- Storage that is the destination of a disaster recovery capable backup connection (to a disaster recovery node)
  - Configuration requirements:  
Volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes). No qtree on same storage system as the primary qtree. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a mirror connection (not disaster recovery capable)
  - Configuration requirements are any of the following:
    - Volume

- Qtree
  - Storage system, or aggregate, containing one of the above
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a disaster recovery capable mirror connection
    - Configuration requirements are all of the following:
      - Volume (possibly containing qtrees), aggregate (possibly containing volumes), *or* an entire storage unit (possibly containing aggregates or volumes)
      - Nothing that is in another dataset
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a mirror connection (not disaster recovery capable)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a disaster recovery capable mirror connection (to a disaster recovery node)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees. No volume on the same storage system as the primary volume. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
    - Storage system licensing requirements: SnapMirror
  - Any node
    - Configuration requirements: Nothing that is in a resource pool used by this dataset
    - Storage system licensing requirements: None
  - Primary (root) node with local backup schedule
    - Configuration requirements: No Open Systems SnapVault directories or Open Systems SnapVault hosts included
    - Storage system licensing requirements: None

- Non-root node
  - Configuration requirements: No Open Systems SnapVault directories or hosts and nothing that is in a non-root node of any other dataset and nothing that is in any node of this dataset.
  - Storage system licensing requirements: None

**Note:**

- If you plan to use SnapMirror with the licensed protection application, you must update the snapmirror.access option in Data ONTAP to specify the destination systems that are allowed to access the primary data source system.  
The snapmirror.access option specifies which SnapMirror destination systems can initiate transfers and which network interfaces they can use. For security reasons, the protection application does not modify the snapmirror.access option for you.
- A single storage system licensed as both SnapVault primary storage and SnapVault secondary storage locations cannot be included in a dataset.
- If you are restoring a LUN, the following points apply:
  - If the protection application is not configured to support non-disruptive LUN restore, the LUN in the destination location must be offline before you start the restore operation.
  - If the protection application is configured to support non-disruptive LUN restore, the LUN in the destination does not have to be offline unless it is owned by a vFiler unit.
  - If the destination LUN is owned by a vFiler unit, non-disruptive LUN restore is not supported.

**Related concepts**

[\*Decisions to make before adding datasets\*](#) on page 711

[\*Decisions to make before adding a resource pool\*](#) on page 837

[\*What a protection policy is\*](#) on page 847

## Volumes unsuitable as mirror destinations

---

Some conditions make a volume unsuitable as a destination for volume SnapMirror-based mirror relationships.

The following conditions make a volume unsuitable as a destination for volume SnapMirror-based mirror relationships:

- More than 10 percent of volume storage space is already in use (as reported by the CLI `df` command).
- More than 10% of volume inodes are already in use (as reported by the CLI `df -i` command).
- The volume contains a qtree which is the root of a vFiler unit.
- Source and destination volumes are running under mismatching versions of Data ONTAP.
- The volume is already serving as a destination for other volume SnapMirror, qtree SnapMirror, or SnapVault relationships.
- The volume is also serving as a source for this volume SnapMirror relationship.
- The potential destination volume is otherwise suitable, but is much larger than the source volume.  
The relationship will work, but space on the destination will be wasted.



# What happens during failover

---

When you start the failover process, the licensed application breaks the SnapMirror relationship between the source storage containers in the primary data node and their destination storage containers in the disaster recovery node and activates the disaster recovery node containers as the active systems that can be accessed by users.

When you invoke failover, the licensed protection application puts the dataset into "failing over" state and carries out the following processes.

1. Runs a failover script (if one is specified by the protection policy) to stop applications writing data to the primary storage systems.
2. Quiesces all SnapMirror related activity between the primary storage systems and their partners in the disaster recovery node.
3. Breaks all SnapMirror relationships between the primary storage systems and their partners in the disaster recovery node.
4. Puts any mirrored LUNs in the online state.
5. Runs a failover script (if one is specified by the protection policy) to restart applications writing data to the secondary systems in the disaster recovery node.
6. Enables the same export protocols (CIFS, NFS, iSCSI, or FCP) for the containers in the disaster recovery node as were enabled for the containers in the primary storage systems.
7. After the above processes are complete, the licensed protection application changes the dataset out of failing over state.

If the above processes complete successfully, the dataset state is changed to "failed over." You can now direct or re-map users to access their data from storage in the disaster recovery node.

If one of the above processes failed, the state is changed to "failover error."



# What failover scripts are

---

If the failover process is invoked, an optional failover script, located on the DataFabric Manager server, specifies tasks, affecting data in primary storage or in disaster recovery node storage, that might need to be completed just before and just after the failover mirror relationship is broken.

**Note:** The **Jobs** window can display up to 2 KB of failover script output for the Mirror Break Script End event. Output exceeding 2 KB is truncated and not recoverable.

## Next topics

[Failover script variables](#) on page 637

[Failover script example](#) on page 638

## Related tasks

[Enabling disaster recovery protection](#) on page 641

## Failover script variables

A failover script can include the following variables that are passed to it from the licensed protection application.

Variable	Description
DP_CONNECTION_ID	A tracking ID generated by the licensed protection application.
DP_DATASET_ID	A tracking ID generated by the licensed protection application.
DP_DATASET_NAME	The name of the dataset to which this script is to be applied.
DP_FAILOVER_SCRIPT_TEST	Whether or not this failover script is being invoked as a test. Starting a test failover by clicking <b>test failover</b> on the Disaster Recovery tab sets this value to 1.
DP_FAILOVER_STATUS	Whether the failover process is currently in the stage before or stage after the failover mirror relationship is broken. Values are either: <ul style="list-style-type: none"> <li>• DP_BEFORE_FAILOVER_MIRROR_BREAK</li> <li>• DP_AFTER_FAILOVER_MIRROR_BREAK</li> </ul>
DP_JOB_ID	A tracking ID generated by the licensed protection application.
DP_POLICY_ID	A tracking ID generated by the licensed protection application.

Variable	Description
DP_POLICY_NAME	The name of the disaster protection policy that is calling this failover script.
DP_SERIAL_NUMBER	The serial number of the DataFabric Manager server software.

## Failover script example

This example script performs prefailover and postfailover tasks.

The following simple example script carries out the following functions:

- Checks to see if the failover is a test failover or an actual failover.
- Sends feedback to be displayed in the Job Summary field of the **Jobs** window.
- Stops a data-producing application prior to the failover mirror relationship break.
- Restarts a data producing application after the failover mirror relationship break.

```
#!/bin/sh
if [ "$DP_FAILOVER_SCRIPT_TEST" = "1" ]
then
    echo This is a TEST failover.
else
    echo This is an ACTUAL failover.
fi
echo Script called with DP_FAILOVER_STATUS=$DP_FAILOVER_STATUS
# Perform different operations based on failover status
case "$DP_FAILOVER_STATUS" in
DP_BEFORE_FAILOVER_MIRROR_BREAK)
    echo "Perform script operations before mirror break."
    # stop MySQL server
    rsh -l user_a r_host1 /etc/rc.d/init.d/mysqld stop
    ;;
DP_AFTER_FAILOVER_MIRROR_BREAK)
    echo "Perform script operations after mirror break."
    # start MySQL server
    rsh -l user_a r_host1 /etc/rc.d/init.d/mysqld start
    ;;
*)
    echo "Unknown DP_FAILOVER_STATUS: $DP_FAILOVER_STATUS"
    exit 1
esac
# Return 0 for success.
# Return 1-255 for failure.
exit 0
```

# Decisions to make before configuring disaster recovery protection

---

Before you configure disaster recovery protection for a dataset, use the following questions to plan your disaster recovery capable dataset and protection policy.

## Next topics

[\*Disaster recovery capable dataset considerations\*](#) on page 639

[\*Disaster recovery protection policy considerations\*](#) on page 640

## Related tasks

[\*Enabling disaster recovery protection\*](#) on page 641

## Disaster recovery capable dataset considerations

When planning the configuration of the datasets on which you want to set up disaster recovery protection, you need to consider the location of your storage nodes, the type of resources on storage nodes, and how you want to assign storage.

**Storage node sites** Are your planned primary storage node and disaster recovery storage node sites located a safe distance from one another?

You should plan to locate the disaster recovery node storage site far enough away from the primary storage site so that it is not affected by any event that can disable the primary site.

**Storage node resources** Are your planned primary storage node and disaster recovery storage node resources, storage systems with SnapMirror installed?

Disaster recovery protection can only be implemented on storage systems installed with SnapMirror and failover features.

**Storage node resource capacity** Do your planned primary and disaster recovery storage node resources match up in capacity and installed applications?

To support continuous user access, successful failover requires that the secondary node storage systems be configured with the same environment settings and applications as those on the primary node storage systems.

- Storage resource assignment** How do you plan to assign resources to your dataset primary and disaster recovery nodes?
- Manual resource assignment (that is, not use a provisioning policy)  
Make sure the resources assigned to the primary and disaster recovery nodes are matched in size and installed applications.
  - Using provisioning policies and resource pools
    - The assigned provisioning policies must specify the application installations, system capacities, and export protocols that will enable a functioning SnapMirror relationship between volumes and qtrees in the primary and disaster recovery nodes.
    - The assigned resource pools must contain storage systems configured to comply with the provisioning policies.

## Disaster recovery protection policy considerations

When configuring a disaster recovery protection policy, you need to consider

- Type of disaster recovery protection policy** What type of disaster recovery protection policy do you plan to provide? The licensed protection application displays a list of six disaster recovery protection policies (each labeled with a DR prefix).
- Failover script** In addition to failover, do you need to perform additional scripted shutdown and restart processes before and after the SnapMirror relationship break is invoked?  
If so, you need to supply and specify a path to a user-created failover script.

# Enabling disaster recovery protection

---

To configure disaster recovery protection you use the licensed application's **Add Protection Policy** wizard, **Add Dataset** wizard, and the **Dataset Policy Change** wizard.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. Select a disaster recovery protection policy.

Use the **Add Protection Policy** wizard to customize a disaster recovery protection policy to apply to your data.

To customize a disaster recovery protection policy, select a base policy with a "DR" prefix. If necessary, write a failover script and specify the path to it.

2. Create a disaster recovery capable dataset.

Use the **Add Dataset** wizard to create a dataset to contain your data.

The wizard guides you to create a single primary node dataset and to provision it, either by directly assigning resources to it, or, if you have a provisioning license installed, by assigning a provisioning policy and resource pool.

3. Create an optional failover script.

If necessary, author a failover script that specifies data application-related tasks that need to be performed before and after the SnapMirror relationship break in the failover process (for example, stopping database writes to primary storage).

4. Assign a disaster recovery capable protection policy to your target dataset.

Use the **Dataset Policy Change** wizard to assign a protection policy to any existing dataset and create and provision any resulting secondary and tertiary nodes.

To make the secondary storage node in this dataset disaster recovery capable, assign it only resources with storage systems with SnapMirror installed.

## After you finish

After enabling disaster recovery protection on a dataset, you can test the failover process and monitor the failover readiness of your disaster recovery enabled datasets.

- To test the optional failover script in the assigned disaster recovery capable protection policy use the Test button on the Disaster Recovery tab.
- To monitor all datasets in your authorized group for failover readiness issues, use the **Failover Readiness** panel in the **Dashboards** window.
- To monitor the failover readiness of specific datasets, check their status in the Failover column of the Disaster Recovery tab.

#### **Related concepts**

[\*Decisions to make before configuring disaster recovery protection\*](#) on page 639

[\*What failover scripts are\*](#) on page 637

#### **Related tasks**

[\*Adding a protection policy\*](#) on page 671

[\*Adding a dataset\*](#) on page 719

[\*Assigning or changing a protection policy\*](#) on page 725

[\*Testing failover scripts\*](#) on page 644

[\*Monitoring failover readiness\*](#) on page 643

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Ensuring disaster recovery readiness

---

If disaster or mishap threatens to disable or destroy primary storage systems in a disaster recovery capable dataset, you can invoke procedures to assess the need for, prepare for, and, if necessary, execute failover processes.

## Next topics

[\*Monitoring failover readiness\*](#) on page 643

[\*Testing failover scripts\*](#) on page 644

## Monitoring failover readiness

You can use the **Failover Readiness** panel to monitor the readiness of your disaster recovery capable datasets to carry out successful failover operation.

### Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Step

1. From the navigation pane, click **Dashboards > Protection > Failover Readiness**.

The protection application displays the Disaster Recovery tab which lists all datasets in the current group and a failover column which displays their current failover statuses.

### After you finish

The datasets that are ready for failover will have a failover status of ready.

### Related tasks

[\*Enabling disaster recovery protection\*](#) on page 641

### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

## Testing failover scripts

If you have a Disaster Recovery license installed, you can use the Disaster Recovery tab to test the operation of your optional user-generated failover scripts without conducting an actual failover.

### Before you begin

- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. start and stop applications on the storage systems of the dataset being tested.
- Ensure that the failover script flags are set to prevent actual failover operations from proceeding.

### Steps

1. From the navigation pane, click **Data ▶ Datasets ▶ Disaster Recovery**.

The licensed protection application lists all the datasets that have been assigned disaster recovery capable protection policies.

2. Select the dataset on which you want to test the failover script and click **Test**.

The licensed application begins testing the failover script that is stored on the associated DataFabric Manager server and specified in the disaster recovery capable protection policy assigned to the selected dataset.

You can monitor the progress of the failover test job in the **Jobs** window.

### Related tasks

[\*Enabling disaster recovery protection\*](#) on page 641

### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Executing disaster procedures

---

If disaster or mishap threatens to disable or destroy primary storage systems in a disaster recovery capable dataset, you can invoke procedures to assess the need for, prepare for, and, if necessary, execute failover processes.

## Next topics

[Disaster management options](#) on page 645

[Updating disaster recovery node storage before failover](#) on page 646

[Starting failover](#) on page 647

[Monitoring failover status](#) on page 648

## Disaster management options

If disaster or mishap jeopardizes the operation of your disaster recovery-capable primary node storage systems, you can use status and event information to assess your backup, failover, or restoration options.

### Events

Path: **Dashboards > Protection > Top Five Events** or **Notifications > Events**

Look for: Hosts down or Volume offline events, which indicate conditions in primary storage that might require failover to storage systems in the disaster recovery node.

### Storage systems status

Path: **Hosts > Storage Systems**

Look for: Storage systems whose System Status column indicates that they are down and might require failover to storage systems in the disaster recovery node. Use the System Status column  button to filter for Down status.

### Disaster recovery failover status

Path: **Data > Datasets > Disaster Recovery**

Look for: The Failover Ready status in the Failover column of the listed disaster recovery capable datasets.

### Disaster recovery failover lag status

Path: **Data > Datasets > Disaster Recovery**

Look for: In Failover Lag status column, whether the last successful backup of primary node data to the disaster recovery node in the listed datasets is satisfactorily current enough for you to invoke failover without a final update.

#### **Failover readiness**

Path: **Dashboards > Protection > Failover Readiness**

Look for: Normal status, which indicates that all disaster recovery capable datasets are ready to undergo failover if necessary.

A Warning or Error status indicates that conditions exist in one or more of your disaster recovery capable datasets that jeopardize successful failover.

#### **Disaster recovery job progress**

Path: **Data > Datasets > Disaster Recovery > Jobs**

Look for: Among other information, the last successful backup or mirror operation (including time started) in a dataset.

## **Updating disaster recovery node storage before failover**

If you have a Disaster Recovery license installed, you can use the Disaster Recovery tab to carry out a final unscheduled Snapshot mirror update from primary to disaster recovery node. You might carry out this operation in anticipation of possible failover operations necessitated by approaching mishap or disaster threatening your primary storage site.

### **Before you begin**

- Ensure that enough time exists before the possible necessity of failover to complete a Snapshot update.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. edit protection schedules.

### **Steps**

1. From the navigation pane, click **Data > Datasets > Disaster Recovery**.
2. Select the dataset on which you might need to execute failover processes.

If the failover lag status displayed for that dataset is Error or Warning, and if you believe you have enough time to complete it, you should complete the steps in this task.

3. Click **Update** then click **Update** again in the confirmation dialog box to confirm your update request.  
The licensed application displays a confirmation prompt.

After the update operation is complete and if you invoke a successful failover process, the disaster recovery node takes over as the functioning primary storage node, which provides users with access to the updated data.

## Related references

[Administrator roles and capabilities](#) on page 1055

# Starting failover

If you have a Disaster Recovery license installed, you can use the Disaster Recovery tab in the licensed protection application to invoke the failover process from primary to secondary storage.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Disaster Recovery tab is not already displayed, from the navigation pane, click **Data ▶ Datasets ▶ Disaster Recovery**.
2. Select the dataset on which you plan to execute failover processes and confirm the failover status for the selected dataset is Ready.

**Note:** If the failover lag status displayed for the dataset is Error or Warning, and if you have enough time, you should update the disaster recovery node storage before failover.

3. Click **Failover**.
4. If you want to check which volumes or qtrees will be affected by failover before executing failover, click **Details** in the confirmation dialog box.

The application lists which Volume SnapMirror or Qtree SnapMirror relationships will be broken, and which destination volumes or qtrees in the disaster recovery node will assume primary storage function.

5. Click **Update** again in the confirmation dialog box to confirm your update request.

The application initiates the failover processes. A successful failover process causes the disaster recovery node site volumes or qtrees to take over and provide primary storage function and availability.

## After you finish

After initiating the failover process, go to the **Failover Status** panel to monitor the progress of the failover operation.

## Related references

[Administrator roles and capabilities](#) on page 1055

## Monitoring failover status

After you start a failover process, you can use the **Failover Status** panel to monitor its progress.

### Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Step

1. From the navigation pane, click **Dashboards** ► **Protection** ► **Failover Status**.

### After you finish

After a successful failover, consider your failback strategies.

### Related concepts

[\*Recovery from disaster\*](#) on page 649

### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Recovery from disaster

---

In the aftermath of a disaster and successful failover, you can assess whether you need to restore primary storage functions to the storage elements on the original primary node and if so, whether those storage elements need data updated from the current functioning primary storage systems.

Possible recovery actions after failover include the following:

- Make the successful failover target node into the new permanent primary storage system  
Maintain the temporary primary storage systems in the disaster recovery node as the permanent primary storage systems.
- Reactivate the original primary node without updating  
Reactivate and resume forward mirroring from the original primary node without updating its original data.
- Resynchronize to undamaged storage in original primary node  
Resynchronize data from the disaster recovery node to the undamaged storage in the original primary node.
- Resynchronize to destroyed and replaced storage in original primary node  
Resynchronize data from the disaster recovery node to the destroyed and replaced storage in the original primary node.

## Next topics

[\*Making the disaster recovery node the new primary data storage\*](#) on page 649

[\*Recovering by resuming forward mirroring\*](#) on page 651

[\*Recovering by resynchronizing data to undestroyed containers\*](#) on page 652

[\*Recovering by resynchronizing data to replaced containers\*](#) on page 654

## Related tasks

[\*Monitoring failover status\*](#) on page 648

## Making the disaster recovery node the new primary data storage

After a successful failover, you have the option of making the disaster recovery node storage, which is currently serving the active data, to be the permanent primary data node.

### Before you begin

- Determine which protection policy you want to assign to the dataset. This policy can be either disaster recovery capable or not.
- Be sure you are familiar with the decisions you must make before assigning or changing policies.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### About this task

After successful failover, to maintain the now active volumes and qtrees in the disaster recovery node as permanent primary storage, reassign the dataset a protection policy (either disaster recovery capable or not) and designate the current disaster recovery node as the new primary data node.

### Steps

1. From the navigation pane, click **Data > Datasets > Overview** tab and then select the failed over dataset.

The Overview tab displays the failed-over dataset with the original primary data node offline and inactive.

2. Click **Protection Policy** to start the **Dataset Policy Change** wizard.
3. When the **Dataset Policy Change** wizard presents the option, click **Yes, abandon the primary nodes resources**.
4. Select a disaster recovery capable protection policy.

You can select among possible node mappings for that protection policy that do not configure the original primary node as the new primary node.

5. Select a node mapping that configures the current disaster recovery node as the new primary node.

**Note:** The usual practice is to select a node mapping that requires the least amount establishing a new baseline of backup or mirror copies.

6. Complete the wizard.

### Related concepts

[\*Decisions to make before adding or changing resource assignments\*](#) on page 735

### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

## Recovering by resuming forward mirroring

After a successful failover, if the original primary storage site is not destroyed and no update of data on the original primary storage site is required, you can use the `dfpm` and `dfdrm` commands on the DataFabric Manager server to restore active primary storage function to the original primary storage node.

### Before you begin

- Confirm that the change you want to make to this protection policy is acceptable for all datasets using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** Necessary capabilities include the ability to restart storage systems on the primary and secondary nodes in the dataset on which you want to resume forward mirroring.

### Steps

- Log in to the DataFabric Manager server to which your licensed protection application is assigned.
- In the command line interface, enter the command:

```
dfpm dataset list -m data_set_name
```

This command finds the primary volumes and qtrees of the specified dataset.

- Enter the command:

```
dfpm dataset list -R
```

This command finds the disaster recovery volume and qtree partners for all primaries. SnapMirror relationships that were broken during the failover are indicated by the "broken\_off" state.

- If your disaster recovery protection policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror resync dr_obj1 dr_obj2 dr_obj3 dr_obj... non_dr_obj1
non_dr_obj2 non_dr_obj3 non_dr_obj...
```

This command reinstates the SnapMirror relationships that were broken during the failover in the disaster recovery node and in the non-disaster recovery secondary node. In this command, `dr_obj...` and `non_dr_obj...` are all volumes and qtrees in either the disaster recovery node or the non-disaster recovery node in "broken\_off" state that you want to restore to "snapmirrored" state.

Wait for all relationships to be in the "snapmirrored" state, then skip to Step 7.

- If your disaster recovery protection policy is based on DR Mirror then Mirror node mappings, enter the command:

```
dfdrm mirror resync dr_obj1 dr_obj2 dr_obj3 dr_obj... tertiary_obj1  
tertiary_obj2 tertiary_obj3 tertiary_obj...
```

This command reinstates the SnapMirror relationships that were broken during failover in the disaster recovery node and the tertiary node. In this command, *dr\_obj...* and *tertiary\_obj...* are all volumes and qtrees in either the disaster recovery node or the tertiary node in "broken\_off" state that you want to restore to "snapmirrored" state.

Wait for all relationships to be in the "snapmirrored" state, then skip to Step 7.

6. In all other cases, enter the command:

```
dfdrm mirror resync dr_obj1 dr_obj2 dr_obj3 dr_obj...
```

This command reinstates the SnapMirror relationships in the disaster recovery node that were broken during failover. In this command, *dr\_obj...* is all disaster recovery node volumes and qtrees in "broken\_off" state that you want to restore to "snapmirrored" state.

Wait for all relationships to be in the "snapmirrored" state before continuing to the next step.

7. Enter the command:

```
dfpm dataset failover state dataset_name ready
```

This command sets the dataset disaster recovery status back to ready.

#### Related references

[Administrator roles and capabilities](#) on page 1055

## Recovering by resynchronizing data to undestroyed containers

After a successful failover, you can use the `dfpm` and `dfdrm` commands on the DataFabric Manager server to restore primary storage function to your original undestroyed primary storage systems and containers and update their data with the most recent changes made to their failover partners in the disaster recovery node.

#### Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

#### Steps

1. Log in to the DataFabric Manager server to which your licensed protection application is assigned.
2. In the command line interface, enter the command:

```
dfpm dataset list -R data_set_name
```

This step finds the secondary storage elements for all primary storage elements. SnapMirror relationships that were broken during the failover are indicated by the "broken\_off" state.

3. If your protection policy is based on the DR Mirror and Mirror node mapping, enter the command:

```
dfdrm mirror break non_dr_obj1 non_dr_obj2 non_dr_obj3 non_dr_obj...
```

This command breaks the SnapMirror relationships between source volumes and qtrees in the primary node and destination volumes and qtrees in the non-disaster recovery node.

Skip to Step 5.

4. If your protection policy is based on the DR Mirror then Mirror node mapping, enter the command:

```
dfdrm mirror break tertiary_obj1 tertiary_obj2 tertiary_obj3 tertiary_obj...
```

This command breaks the SnapMirror relationships between source volumes and qtrees in the disaster recovery node and destination volumes and qtrees in the tertiary node.

5. Enter the command:

```
dfdrm mirror resync -r dr_obj1 dr_obj2 dr_obj3 dr_obj...
```

This command temporarily reverses the original SnapMirror relationships (which updates the original primary storage containers as SnapMirror destinations).

In this command, *dr\_obj...* is all volumes and qtrees in the disaster recovery node, now serving as primary storage, that you want to temporarily configure as a SnapMirror sources.

Wait for all relationships to be in the "snapmirrored" state before continuing to the next Step.

6. Enter the command:

```
dfdrm mirror break original_obj1 original_obj2 original_obj3 original_obj...
```

This command quiesces and breaks the temporary reversed mirror relationships.

In this command, *original\_obj...* is all original primary objects that are temporarily configured as SnapMirror destinations.

7. After you break the reversed mirror relationship, inspect the data on the original primary objects to verify validity.

8. Enter the command:

```
dfdrm mirror resync -r original_obj1 original_obj2 original_obj3  
original_obj...
```

This command resyncs the mirror copies to reestablish the original SnapMirror relationships (in other words, to reverse the relationships back to forward mirror).

9. If your protection policy is based on the DR Mirror and Mirror node mapping, enter the command:

```
dfdrm mirror resync non_dr_obj1 non_dr_obj2 non_dr_obj3 non_dr_obj...
```

This command resyncs the mirror copies to reestablish the original primary node to non-disaster recovery secondary node SnapMirror relationships.

Skip to Step 11.

- 10.** If your protection policy is based on the DR Mirror then Mirror node mapping, enter the command:

```
dfdrm mirror resync tertiary_obj1 tertiary_obj2 tertiary_obj3  
tertiary_obj...
```

This command resyncs the mirror copies to reestablish the original disaster recovery node to tertiary node SnapMirror relationships.

- 11.** Confirm the success of the resync operation by noting its job list ID output and entering the command:

```
dfdrm job list joblist_id
```

If the job list command indicates a resync job failure, then reinitialize the mirror relationship between each volume or qtree by using the command

```
dfdrm mirror initialize dr_obj tertiary_obj
```

- 12.** Enter the command:

```
dfpm dataset failover state dataset-name ready
```

This command sets the dataset disaster recovery state to ready.

#### Related concepts

[Fallback options](#) on page 587

#### Related references

[Administrator roles and capabilities](#) on page 1055

## Recovering by resynchronizing data to replaced containers

After a successful failover, you can use the dfpm and dfdrm commands on the DataFabric Manager server to restore primary storage function to destroyed and replaced original primary storage containers and resynchronize primary storage data with the most recent updates.

#### Before you begin

- At the original primary storage site, confirm that the destroyed storage systems, aggregates, volumes, and qtrees are replaced with containers of the same name, capacity, and configuration.

**Note:** Configure the replacement volumes in restricted (not online or offline) state.

- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. Log in to the DataFabric Manager server to which your licensed protection application is assigned.
2. In the command line interface, enter the command:

```
dfpm dataset list -R data_set_name
```

This step finds the secondary storage elements for all primary storage elements. SnapMirror relationships that were broken during the failover are indicated by the "broken\_off" state.

3. Enter the command:

```
dfpm dataset list -m -M data_set_name
```

This step lists the missing (destroyed) containers in the specified dataset.

4. After listing the missing containers, in each system with a missing container, use FilerView or the Data ONTAP CLI to recreate the missing aggregates, volumes, or qtrees. Configure the replacement volumes with restricted (not online or offline) state.
5. If your disaster recovery protection policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror delete non_dr_obj1
```

This step deletes the non-disaster recovery node mirror destination objects.

6. Enter the command:

```
dfdrm mirror initialize dr_obj_name1 replaced_obj_name
```

This command creates a new SnapMirror relationship to the replacement volumes and qtrees in the original primary node from their source partner volumes and qtrees in the disaster recovery node. It temporarily configures the disaster recovery node volumes and qtrees as SnapMirror source objects and the replacement volumes and qtrees as destination objects. It then copies the updated data from the volumes and qtrees in the disaster recovery node to the replacement volumes and qtrees in the original primary node.

**Note:** Because you cannot create a SnapMirror relationship to a replacement aggregate, use this command to create SnapMirror relationships to that aggregate's child volumes instead.

7. Repeat Step 6 for each disaster recovery node volume or qtree that has a replacement volume or qtree.
8. After the mirror initialize operations are complete, enter the command:

```
dfdrm mirror quiesce replaced_obj1 replaced_obj2 replaced_obj3  
replaced_obj...
```

This step quiesces these new mirror relationships prior to breaking and reversing them. In this command, *replaced\_obj...* is all the replacement containers that you have just updated.

**9.** Enter the command:

```
dfdrm mirror break replaced_obj1 replaced_obj2 replaced_obj3 replaced_obj...
```

This command breaks the current mirror relationships prior to reversing them.

**10.** After you break the mirror relationship, inspect the data on the original primary objects to verify validity.

**11.** Enter the command:

```
dfdrm mirror resync -r replaced_obj1replaced_obj2  
replaced_obj3replaced_obj...  
to reverse the mirror relationship.
```

This action establishes the replacement volumes and qtrees as the primary storage containers and the volumes and qtrees in the disaster recovery node as the SnapMirror destination objects.

**12.** If your disaster recovery protection policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror initialize replaced_obj...non_dr_obj...
```

This command creates a new SnapMirror relationship between the replacement volumes and qtrees in the original primary node and their partner volumes and qtrees in the non-disaster recovery node. It temporarily configures the disaster recovery node volumes and qtrees as SnapMirror source objects and the replacement volumes and qtrees as destination objects.

Repeat this command for each replaced volume or qtree in the primary node.

**13.** If your disaster recovery policy is based on DR Mirror and Mirror node mappings, enter the command:

```
dfdrm mirror resyncnon_dr_obj1non_dr_obj2non_dr_obj..non_dr_obj3
```

This command updates the empty volumes and qtrees in the non-disaster recovery node with data from their replaced partners in the primary node. In this command, *non\_dr\_obj...* is all the volumes and qtrees in the non-disaster recovery node that you want to update.

Wait for all relationships to be in the "snapmirrored" state.

**14.** Enter the command:

```
dfpm dataset replace dataset-name
```

This command replaces the dataset reference to old primary volumes and qtrees with replaced volumes and qtrees.

**Note:** This step carries out replacement of old with new volume and qtree references only. To replace old with new aggregate references in the failed back dataset, see the next step.

- 15.** If the failed-back dataset originally included aggregates, complete the following commands to add reference to the replacement aggregates and delete reference to their child volumes in the failed-back dataset.

Even though the failed aggregate was destroyed and replaced, you still need to complete the following steps to reference the replacement aggregate in the failed-back dataset.

- a. Enter the command:

```
dfpm dataset list -m dataset_name
```

This command lists the child members (volumes or qtrees) of the replacement aggregate.

- b. Enter the command:

```
dfpm dataset remove dataset_name child_obj
```

This command removes reference to the child members of the replacement aggregates from this dataset.

Even though references to the child replacement volumes are removed from the dataset, the SnapMirror relationships and operations between these replacement volumes and their disaster recovery node mirrors remain intact.

- c. Enter the command:

```
dfm aggr list storage_system
```

This command lists the replacement aggregate at the primary site.

- d. Enter the command:

```
dfpm dataset add dataset_name replacement_aggr
```

This command adds the replacement aggregate to the failed back dataset.

- e. Enter the command:

```
dfpm dataset list -m dataset_name
```

This command confirms the addition of the replacement aggregate to this dataset by listing the dataset contents.

- 16.** Enter the command:

```
dfpm dataset list -R dataset_name
```

This step confirms the disaster recovery relationship between the replacement child volumes and their destinations in the disaster recovery node.

- 17.** Enter the command:

```
dfpm dataset failover state dataset_name ready
```

This step sets the dataset disaster recovery state to ready.

**Related concepts**

[\*Fallback options\*](#) on page 587

**Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Data > Datasets > Disaster Recovery

---

You can use the Disaster Recovery tab to perform monitoring, update, testing, and failover tasks on datasets if you have installed the Disaster Recovery license.

- [Command buttons](#) on page 659
- [Datasets list](#) on page 659
- [Graph tab](#) on page 660
- [Jobs tab](#) on page 662
- [Window customization](#) on page 663

## Command buttons

<b>Failover</b>	Starts the process for primary-to-disaster recovery node failover in the selected disaster recovery enabled dataset.
<b>Test</b>	Tests the validity of user-defined failover scripts specified in the disaster recovery protection policy that is assigned to the selected dataset.
<b>Update</b>	Starts an immediate primary-to-disaster recovery node update in the selected dataset.  This operation is most likely invoked in preparation for an impending event that can potentially disable a primary storage facility and necessitate failover to a disaster recovery-enabled backup site, but is still distant enough to allow completion of a final backup of data from a primary storage node to its disaster recovery-enabled node.
<b>Cancel</b>	Cancels any update or failover operation in the selected dataset.

## Datasets list

Displays a table of all datasets enabled for disaster recovery protection.

<b>Name</b>	The name of the dataset.
<b>Failover</b>	The failover status of the dataset. Possible statuses include the following:
<b>Ready</b>	The dataset is ready for failover.
<b>Failing over</b>	The dataset is in the process of failover.
<b>Failed over</b>	The dataset has completed successful failover.
<b>Failed over - Warning</b>	The dataset completed failover with warnings.
<b>Failed over - Error</b>	The dataset encountered errors during failover. Failover is not successful.

**Failover** The current status of the data backup between the primary data node and the disaster recovery node. Valid values, in alphabetical order, are as follows:

<b>Baseline Failed</b>	The dataset's initial baseline transfer did not succeed. Check the conformance status for more information.
<b>Initializing</b>	The dataset is in conforming state (becoming conformant) and its initial baseline transfer is taking place.
<b>Job Failure</b>	The most recent protection operation for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded the lag error threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>Lag Warning</b>	The dataset has reached or exceeded the lag warning threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>No Protection Policy</b>	The dataset is managed by the protection application, but no protection policy has been assigned to the dataset.
<b>Protected</b>	The data is being protected according to policy.
<b>Protection Suspended</b>	All protection operations between the primary node and disaster recovery node have been suspended.
<b>Uninitialized</b>	The dataset does not have any data in it, or it has only one node and its assigned policy has no schedule configured, or it has only one node and the backup Snapshot copy schedule for the assigned policy has not started any jobs.

**Description** A description of the dataset.

## Graph tab

Displays a selectable topological representation of the primary node, disaster recovery node, backup connections, and any other secondary node assigned to the selected dataset. Clicking a node or connection displays failover status and resource information about that node that you might need to evaluate prior to starting failover.

**Status**

<b>Primary Data node details</b>	If the primary storage node is selected, the licensed protection application displays the following primary storage node data:
<b>Protection</b>	The status of the data protection scheme assigned to this dataset (protected, uninitialized, suspended, lag warning, or lag error).
<b>Conformance</b>	Whether or not provisioning conformance errors exist in the selected node. If error conditions exist, click  for details.
<b>Resource</b>	Whether or not error or critical conditions exist in the resources assigned to the selected node.
<b>Space</b>	Whether or not space issues exist on the selected node. If warning or error conditions exist, click  for details.
<b>Failover</b>	The failover state of the primary data node.
<b>Physical resources</b>	Listing of the physical systems assigned to the selected node. Click  for details.
<b>Resource pools</b>	Resource pools, if any, that are assigned to provision the selected node.
<b>Local backup schedule</b>	The name of the local backup schedule, if any, that is assigned to the selected node. Click  for a graphical display of the exact backup times.
<b>Backup versions</b>	Listing of Snapshot copies stored on this node.
<b>Dataset properties details</b>	Depending on the properties of the selected dataset, the licensed protection application displays some or all of the following details.
<b>Owner</b>	Owner of the current dataset.
<b>Contact</b>	E-mail contact address for this dataset.
<b>Time zone</b>	Time zone in which the dataset is located.
<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.
<b>Application version</b>	(Displayed for application datasets) The application version that generated the dataset.
<b>Application server</b>	(Displayed for application datasets) The name of the application server that generated the dataset.

**Connection details** If the connection element is selected, Protection Manager displays the following data in connection with the data protection connections:

<b>Relationships</b>	The protection relationships between a source and target nodes.
<b>Schedules</b>	The name of the protection schedule assigned to this protection connection.
<b>Throttle</b>	The name of the throttle schedule assigned to this protection connection.
<b>Lag status</b>	The current lag status (good, warning, or error) of successfully completed protection backup or mirror operations between the source and target nodes. If error or warning conditions exist, click  for details.

**Backup Node** If the backup node is selected, Protection Manager displays the following data in connection with the data protection backup node:

<b>Node name</b>	The default or user-assigned name of the backup node.
<b>Provisioning policy</b>	The provisioning policy, if any, that is assigned to the backup node.
<b>Physical resources</b>	The physical resources assigned to the selected node. Click  for details.
<b>Resource pools</b>	The resource pools, if any assigned to the selected node. Click  for details.

## Jobs tab

Displays a log listing of the disaster recovery update and failover operations initiated on this dataset.

<b>Job</b>	A list of the jobs related to disaster recovery-related protection configuration or execution that the protection application has executed.
<b>Step</b>	A list of the phases or milestones that occurred or were attempted during the execution of the listed jobs.
<b>Time stamp</b>	The times and dates that the listed jobs and steps started or occurred.
<b>Result</b>	The Normal, Warning, or Error result status of the listed jobs or steps.

**Note:** You can select each listed job or step to display further details on that job or step in the pane to the right.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Dashboards > Protection > Failover Readiness

You can use the **Failover Readiness** panel to view the readiness of datasets configured for disaster recovery protection to successfully carry out failover operations should failover operations become necessary. The panel lists the number of datasets whose failover support configurations are in ready state, warning state, and error state.

## Status Descriptions

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

<b>Failover Readiness</b>	The <b>Failover Readiness</b> panel only appears when the disaster recovery option is licensed. <ul style="list-style-type: none"><li>• Status: Normal Indicates that conditions in all datasets that are configured for disaster recovery protection will support successful failover operations if such operations become necessary. Nothing has changed in the configuration since the dataset was configured for disaster recovery.</li><li>• Status: Warning Indicates that conditions have changed in one or more datasets that are configured for disaster recovery protection so that failover operations might not be completely successful, if such operations become necessary. The datasets producing the warnings should be investigated and brought back into the Normal state.</li><li>• Status: Error Indicates that conditions have significantly changed in one or more datasets that have been configured for disaster recovery protection so that it is likely that failover operations will not be completely successful, if such operations become necessary, and data could be lost. The datasets producing the warnings should be investigated and brought back into the Normal state.</li></ul>
<b>Ready</b>	Total number of datasets that have been configured for disaster recovery protection whose conditions will support successful failover operations, if such operations become necessary.
<b>Ready - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection whose conditions might not support completely successful failover operations, if such operations become necessary.
<b>Error - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection to which significant changes have occurred to the configurations. Failover operations

can still occur but might not be completely successful, if such operations become necessary.

**Total Datasets** The total datasets that have been configured for disaster recovery protection.

Click  beside the dashboard panel title to replace the work area with the Disaster Recovery tab on the **Datasets** window.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.

# Dashboards > Protection > Failover Status

---

You can use the **Failover Status** panel to view the status of an in-progress failover operation. The panel appears when a failover operation is invoked, listing the number of datasets in the process of failing over and the number of datasets that have successfully failed over.

## Status Descriptions

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

<b>Failover Status</b>	The <b>Failover Status</b> panel only appears when the disaster recovery option is licensed. <ul style="list-style-type: none"><li>• Status: Normal. Indicates that failover operations are either successfully completed or are proceeding as expected in all datasets that have been configured for disaster recovery protection.</li><li>• Status: Warning Indicates that failover operations have completed with a warning condition in one or more of the datasets that have been configured for disaster recovery protection.</li><li>• Status: Error Indicates that failover operations have completed with an error condition in one or more of the datasets that have been configured for disaster recovery protection.</li></ul>
<b>Failing over</b>	Total number of datasets that have been configured for disaster recovery protection that are currently undergoing failover operations.
<b>Failed over</b>	Total number of datasets that have been configured for disaster recovery protection that have successfully completed failover operations.
<b>Failed over - Warnings</b>	Total number of datasets that have been configured for disaster recovery protection that have completed failover operations with warning conditions. Warnings can be encountered during the failover operation or warnings that exists in the ready state, as shown in the Failover Readiness panel, can be propagated to the Failed Over state.
<b>Failed over - Errors</b>	Total number of datasets that have been configured for disaster recovery protection that have completed failover operations with error conditions. Errors can be encountered during the failover operation or errors that exists in the ready state, as shown in the Failover Readiness panel, can be propagated to the Failed Over state.

**Total Datasets** The total datasets that are issuing failover status events.

Click  beside the dashboard panel title to replace the work area with the Disaster Recovery tab on the **Datasets** window.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.

# **Protection policies (not disaster recovery capable)**

Protection policies are the backup instructions that you assign to your datasets. These policies describe the type of backup to carry out, the Snapshot copy retention count, what preconfigured Snapshot copy, backup, and throttle schedule to follow, and what scripts to execute. The same policy can be assigned to multiple datasets.

The licensed protection application provides templates for you to configure the following types of backup setups:

**Note:** If the Disaster Recovery feature is licensed on your protection server, additional disaster recovery capable protection policies are available.

<b>Back up</b>	A dataset is backed up locally and also backed up from primary storage to secondary storage on a SnapVault or SnapMirror storage system.
<b>Back up, then Mirror</b>	A dataset is backed up from primary storage to secondary storage on a SnapVault or SnapMirror storage system and from there mirrored to a SnapMirror partner.
<b>Mirror then Mirror</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and from there mirrored to an additional SnapMirror partner.
<b>Local Snapshot copies only</b>	A dataset uses only local Snapshot copies in primary storage to protect data. No backup to secondary storage is implemented.
<b>Mirror</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner.
<b>Mirror and back up</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and is also backed up to secondary storage on a SnapVault or SnapMirror storage system.
<b>Mirror and mirror</b>	A dataset is mirrored from primary storage to secondary storage on two different SnapMirror partners
<b>Mirror then back up</b>	A dataset is mirrored from primary storage to secondary storage on a SnapMirror partner and from there backed up to tertiary storage on a SnapVault or SnapMirror storage system.
<b>No protection</b>	A dataset is left with no Snapshot copies, backups, or mirror-copy protection of any kind.
<b>Remote backup only</b>	Data on a storage system is backed up remotely to secondary storage on a SnapVault or SnapMirror storage system. The licensed application carries out no local backup on the primary storage. This is the protection policy to assign to third party systems with Open Systems SnapVault installed.

**Related concepts**

*What a protection policy is* on page 847

**Related references**

*Disaster recovery capable protection policies* on page 627

*Disaster recovery capable protection policies* on page 627

# Adding a protection policy

---

You can use the **Add Protection Policy** wizard to create new protection policies. After you create a protection policy, you can apply it to datasets to manage the backup or mirror operations that are executed on those datasets.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the information available that you need to complete this task:

- Policy name, base configuration, name for each node
- Primary node information
- Backup or mirror connection information:
- Backup or mirror node information:

## Steps

1. From the navigation pane, click **Policies > Protection > Overview**.
2. Click **Add** to start the **Add Protection Policy** wizard.
3. Type a policy name and description and click **Next**.
4. Select a base policy and click **Next**.
5. Complete the policy property sheets for the primary node and any backup connection, mirror connection, secondary storage, or tertiary storage node that is required for the policy. After you complete each property sheet, click **Next**.

After all property sheets are completed, the **Add Protection Policy** wizard displays a summary sheet for the policy.

6. Confirm the details of the policy and click **Finish**.

Your new policy is listed on the **Protection Policies** window Overview tab.

## Related concepts

*Decisions to make before adding a protection policy* on page 251

## Related tasks

*Enabling disaster recovery protection* on page 641

## Related references

*Administrator roles and capabilities* on page 1055



# Adding a dataset

---

You can add a dataset to manage protection for data sharing the same protection requirements, or to manage provisioning for the dataset members.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
  - Provisioning policy for nonprimary dataset nodes
- If you plan to assign a policy, you need to be assigned a role that enables you to view policies.
- If you plan to assign a provisioning policy, you also need a role that enables you to attach the resource pools configured for the policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Datasets ▶ Overview**.
2. Click **Add** to start the **Add Dataset** wizard.

If you want to provision your node by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.

**Note:** If you receive a message that the maximum number of vFiler units has been reached, you must relinquish the migration capability for one or more datasets before you can configure an IP address and network mask that enables the migration capability for a dataset.

3. Complete the steps in the wizard to create a dataset.

If you have the protection license and you did not assign a protection policy to the dataset or assign resources to each destination node when creating the new dataset, the data is not yet protected.

If you have the provisioning license and you did not assign a provisioning policy to each of the dataset nodes, you will have to manually provision each node.

If you have the disaster recovery license and you did not assign a disaster recovery policy to the dataset, the data is not protected for disaster recovery.

#### **Related concepts**

*[Decisions to make before adding datasets](#)* on page 711

*[Effect of time zones on schedules](#)* on page 1049

#### **Related tasks**

*[Relinquishing migration capability of a dataset](#)* on page 797

*[How do I back up data?](#)* on page 589

*[Enabling disaster recovery protection](#)* on page 641

#### **Related references**

*[Dataset properties](#)* on page 709

*[Administrator roles and capabilities](#)* on page 1055

# Assigning or changing a protection policy

---

You can assign a policy to a dataset or change the policy assigned to it. The policy specifies how the data is to be protected.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Determine which policy you want to assign to the dataset. You can review available protection policies on the **Protection Policies** window. If no policy meets the requirements of your new dataset, you can create a new policy or modify a copy of an existing policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can use this procedure after you have created a new dataset and want to assign a policy to it, or when you want to change the protection policy assigned to a dataset. You can also use this procedure to protect a dataset that is listed on the **Datasets** window.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select a dataset and click **Protection Policy** to start the **Dataset Policy Change** wizard.  
**Note:** If you want to provision your nodes by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.
3. Complete the steps in the wizard.

## Related concepts

[\*Decisions to make before assigning or changing policies\*](#) on page 721

[\*What a protection policy is\*](#) on page 847

**Related tasks**

*How do I back up data?* on page 589

*Enabling disaster recovery protection* on page 641

**Related references**

*Administrator roles and capabilities* on page 1055

# Administrator roles and capabilities

---

The administrator roles determine the tasks you can perform using applications in NetApp Management Console .

## Default and custom roles

One or more capabilities must be specified for every role, and you can assign multiple capabilities if you want the administrator to have more control than a specific role provides. For example, if you want an administrator to perform both the backup and restore operations, you must assign Back Up and Restore roles to the administrator.

The DataFabric Manager server and the client applications provide a set of default global roles described in the following list. You can customize these roles and the capabilities associated with them and you can create new ones using the Operations Manager Web-based user interface. For more information about configuring role-based access control (RBAC), see the *Operations Manager Administration Guide* .

<b>GlobalBackup</b>	You can initiate a backup to any secondary volume and ignore discovered hosts.
<b>GlobalDataProtection</b>	You can initiate a backup to any secondary volume; view backup configurations, events and alerts, and replication or failover policies; and import relationships into datasets.
<b>GlobalDataset</b>	You can create, modify, and delete datasets.
<b>GlobalDelete</b>	You can delete information in the DataFabric Manager server database, including groups and members of a group, monitored objects, custom views, primary and secondary storage systems, and backup relationships, schedules, and retention policies.
<b>GlobalEvent</b>	You can view, acknowledge, and delete events and alerts.
<b>GlobalFullControl</b>	You can view and perform any operation on any object in the DataFabric Manager server database and configure administrator accounts. You cannot apply this role to accounts with group access control.
<b>GlobalMirror</b>	You can create, destroy, and can update replication or failover policies.
<b>GlobalRead</b>	You can view the DataFabric Manager server database, backup and provisioning configurations, events and alerts, performance data, and policies.
<b>GlobalRestore</b>	You can restore the primary data back to a point in time or restore to a new location.
<b>GlobalWrite</b>	You can view or write to the DataFabric Manager server database.

<b>GlobalResourceControl</b>	You can add members to dataset nodes that are configured with provisioning policies.
<b>GlobalProvisioning</b>	You can provision primary dataset nodes and can attach resource pools to secondary or tertiary dataset nodes. The GlobalProvisioning role also includes all the capabilities of the GlobalResourceControl, GlobalRead, and GlobalDataset roles for dataset nodes that are configured with provisioning policies.
<b>GlobalPerfManagement</b>	You can manage views, event thresholds, and alarms apart from viewing performance information in Performance Advisor.

### Related concepts

[Strategies for enabling a dataset for migration](#) on page 779

### Related tasks

[Printing Help topics](#) on page 111

[Adding alarms](#) on page 601

[Testing alarms](#) on page 87

[Editing alarms](#) on page 89

[Deleting alarms](#) on page 91

[Responding to alarms](#) on page 95

[Monitoring alarms](#) on page 97

[Enabling and disabling alarms](#) on page 99

[Monitoring events](#) on page 65

[Responding to and acknowledging events](#) on page 67

[Deleting events](#) on page 69

[Adding a dataset](#) on page 719

[Assigning or changing a protection policy](#) on page 725

[Provisioning resources for a primary dataset node](#) on page 731

[Changing dataset node resource assignments](#) on page 739

[Adding resources to a dataset](#) on page 737

[Adding resources to a dataset](#) on page 737

[Changing dataset node resource assignments](#) on page 739

[Removing resources from a dataset](#) on page 741

[Editing dataset general properties](#) on page 753

[Deleting a dataset](#) on page 755

[Adding a resource pool](#) on page 841

[Editing resource pool properties](#) on page 845

[Adding groups](#) on page 461

[Editing groups](#) on page 463

*Deleting groups* on page 465  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943  
*Updating Open Systems SnapVault client data* on page 945  
*Diagnosing a storage system* on page 947  
*Diagnosing an Open Systems SnapVault host* on page 949  
*Adding a daily protection schedule* on page 307  
*Adding a weekly protection schedule* on page 309  
*Adding a monthly protection schedule* on page 311  
*Adding a throttle schedule* on page 313  
*Deleting a protection or throttle schedule* on page 323  
*Assigning or changing schedules in a protection policy* on page 325  
*Copying a protection or throttle schedule* on page 327  
*Monitoring dataset status* on page 403  
*Monitoring backup and mirror relationships* on page 405  
*Backing up datasets on-demand* on page 407  
*Suspending protection of datasets* on page 409  
*Suspending data protection for backup volume maintenance* on page 411  
*Resuming protection of datasets* on page 413  
*Restoring backed-up data to a new location* on page 423  
*Restoring backed-up data over current data* on page 425  
*Restoring selected portions of a dataset* on page 427  
*Restoring a virtual machine to its original location* on page 429  
*Restoring a virtual machine file system to any location* on page 431  
*Restoring a virtual machine to its original location through another ESX server* on page 433  
*Importing discovered external relationships* on page 451  
*Adding unprotected host data to an existing dataset* on page 443  
*Adding unprotected host data to a new dataset* on page 445  
*Protecting unprotected datasets* on page 447  
*Starting a vFiler unit migration* on page 961  
*Updating vFiler unit migration SnapMirror relationships* on page 963  
*Cutting over to the new vFiler unit destination* on page 965  
*Cleaning up a vFiler unit migration* on page 967

*Cancelling a vFiler unit migration* on page 969  
*Viewing vFiler unit migration status* on page 971  
*Adding a protection policy* on page 671  
*Editing a policy's primary data node* on page 258  
*Editing a policy's backup connection* on page 259  
*Editing a policy's backup node* on page 260  
*Editing a policy's mirror connection* on page 260  
*Editing a policy's mirror node* on page 261  
*Changing retention times in a protection policy* on page 265  
*Changing lag thresholds in a protection policy* on page 267  
*Changing a node name in a policy* on page 269  
*Deleting a protection policy* on page 271  
*Editing a daily schedule* on page 315  
*Editing a weekly schedule* on page 317  
*Editing a monthly schedule* on page 319  
*Editing a throttle schedule* on page 321  
*Assigning or changing a provisioning policy* on page 727  
*Configuring dataset nodes for NFS protocol access* on page 747  
*Configuring dataset nodes for CIFS protocol access* on page 745  
*Configuring dataset nodes for FC protocol access* on page 749  
*Configuring dataset nodes for iSCSI protocol access* on page 751  
*Displaying export properties for a specific dataset member* on page 417  
*Displaying export and mapping information for all members of a dataset node* on page 415  
*Monitoring failover readiness* on page 643  
*Testing failover scripts* on page 644  
*Updating disaster recovery node storage before failover* on page 646  
*Starting failover* on page 647  
*Monitoring failover status* on page 648  
*Making the disaster recovery node the new primary data storage* on page 649  
*Recovering by resuming forward mirroring* on page 651  
*Recovering by resynchronizing data to undestroyed containers* on page 652  
*Recovering by resynchronizing data to replaced containers* on page 654  
*Testing failover scripts* on page 644  
*Enabling disaster recovery protection* on page 641  
*Adding a dataset* on page 719  
*Configuring dataset nodes for CIFS protocol access* on page 745  
*Configuring dataset nodes for NFS protocol access* on page 747  
*Configuring dataset nodes for iSCSI protocol access* on page 751  
*Configuring dataset nodes for FC protocol access* on page 749

*Assigning or changing a protection policy* on page 725  
*Provisioning resources for a primary dataset node* on page 731  
*Changing dataset node resource assignments* on page 739  
*Adding resources to a dataset* on page 737  
*Removing resources from a dataset* on page 741  
*Editing dataset general properties* on page 753  
*Deleting a dataset* on page 755  
*Viewing volume, LUN or qtree space allocation* on page 757  
*Diagnosing volume or qtree space status* on page 759  
*Diagnosing volume or qtree space status* on page 759  
*Resizing volume space* on page 761  
*Resizing qtree space* on page 763  
*Deleting Snapshot copies* on page 765  
*Deleting a volume, LUN or qtree* on page 767  
*Enabling deduplication on your dataset nodes* on page 809  
*Disabling deduplication on dataset nodes* on page 811  
*Starting on-demand deduplication* on page 813  
*Stopping an in-progress deduplication* on page 815  
*Viewing volume-level deduplication space-saving* on page 817  
*Adding a resource pool* on page 841  
*Editing resource pool properties* on page 845  
*Viewing a provisioning policy* on page 859  
*Adding a provisioning policy* on page 875  
*Editing a provisioning policy* on page 879  
*Copying a provisioning policy* on page 881  
*Deleting a provisioning policy* on page 883  
*Viewing vFiler templates* on page 889  
*Adding a vFiler template* on page 893  
*Editing a vFiler template* on page 895  
*Copying a vFiler template* on page 897  
*Deleting a vFiler template* on page 899  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943

- Updating Open Systems SnapVault client data* on page 945
- Diagnosing a storage system* on page 947
- Diagnosing an Open Systems SnapVault host* on page 949
- Monitoring jobs* on page 973
- Cancelling jobs* on page 975
- Starting a dataset migration* on page 783
- Updating dataset migration SnapMirror relationships* on page 785
- Cutting over to the new dataset storage destination* on page 787
- Cleaning up a dataset migration* on page 789
- Relinquishing migration capability of a dataset* on page 797
- Cancelling a dataset migration* on page 791
- Viewing dataset migration status* on page 793
- Assigning or changing a provisioning policy* on page 727

#### **Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Decisions to make before adding or changing resource assignments

---

Before you add or change the physical resources assigned to an existing dataset node, you need to gather the required information.

- For each node in the dataset, which resource pool meets its protection or provisioning requirements? For example, if you have the protection license, the resource pool you assign to a mirror node should contain physical resources that are appropriate for mirrored copies of the dataset. If you have the provisioning license, the resource pool you assign to a dataset node should contain physical resources that are appropriate and large enough for the provisioning needs of the data contained in the dataset node.
- What if there are no resource pools that meet the protection or provisioning requirements of the dataset node? If no resource pool meets the protection or provisioning requirements of a dataset node, you can use the **Resource Pools** window to create a new resource pool for each node.
- If you have the protection and disaster recovery license, can you choose not to use resource pools? You can select physical resources for the backup and mirror nodes of your dataset. If you choose to select storage outside of a resource pool, the licensed protection application does not create volumes but instead uses the volumes you select for that dataset node.
- If you have the provisioning or disaster recovery license, can you choose not to use resource pools? You can manually provision your dataset. If you choose to provision your dataset on storage outside of a resource pool, the licensed provisioning application does not create volumes but instead uses the volumes that you select for that dataset node.

**Note:** If you choose to associate a vFiler unit with a nonprimary node in a dataset, any volumes that are provisioned for that dataset must be associated with the vFiler unit. Therefore, when you view a list of the dataset volumes, only volumes that are owned by the vFiler are displayed.

## Related tasks

[Making the disaster recovery node the new primary data storage](#) on page 649



# What Provisioning Manager is

---

Provisioning Manager helps you simplify and automate the tasks of provisioning and managing storage for the data in datasets.

The licensed provisioning application provides the following capabilities:

- Provisioning policies that manage provisioning and exporting of storage
- Automatic provisioning of a dataset when you assign a provisioning policy to it
- Periodic checking of provisioned storage for conformance to the policy
- Manual controls for adding volumes or qtrees to a dataset on existing storage and newly provisioned storage
- Manual controls for resizing volumes and for deleting old Snapshot copies on existing storage and newly provisioned storage
- Migration of datasets and vFiler units to new storage systems
- Deduplication to eliminate duplicate data blocks to reduce storage space

To enable the provisioning features, you must purchase the provisioning license and install it on DataFabric Manager.

**Note:** If AutoSupport is enabled for DataFabric Manager, weekly AutoSupport messages with the following data are sent to the AutoSupport center:

- Provisioning application license information
- Counts for nodes, datasets, resource pools, provisioning policies, primary provisioning requests (submitted and serviced since the current provisioning application update), and manual space management requests
- Dataset names, associated resource pools, and associated vFiler units
- Dataset nodes associated with provisioning policies



# About the NetApp Management Console dashboards

---

The dashboards provide a broad overview of various aspects of your data management environment.

If you are running more than one data management application, the specific dashboard panels that are displayed change according to the application that is currently selected.

**Protection dashboard** If you have the licensed protection application installed and you select the Protection dashboard, you can determine the current overall protection status of your systems,

such as the number of protected datasets versus unprotected datasets, system events to be addressed, and so forth. You can also gather data for evaluating system actions and to assist in determining how to set up datasets, resource pools, policies, and schedules for the future. If you installed and licensed the disaster recovery option, failover dashboard information is also displayed.

**Provisioning dashboard** If you have the licensed provisioning application installed and you select the Provisioning dashboard, you can determine the current overall status of dataset and resource pool provisioning. In addition to listing the top five events, information provided for datasets includes conformance status, resource status, and space status,

and information provided for resource pools includes space status and overall utilization. This information can help you determine when you need to increase available space for your datasets or when you need to investigate out-of-conformance issues.

**Performance dashboard** If you select **Monitor > Dashboard** in Performance Advisor, the default setting displays information about the current overall performance status of your systems,

such as top performance events, top storage systems by the total number of operations, top storage systems by network throughput, and storage systems by CPU utilization. If you have the proper permissions, you can modify the default settings to configure any view on the global group as a dashboard.

To access an application dashboard, you must have appropriate privileges. Items that you do not have privileges for are not displayed in the dashboard. If you encounter access problems, contact the administrator who maintains your DataFabric Manager roles and privileges.

You can filter the content of the Protection and Provisioning dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.

Information about the dashboard can be viewed by clicking the Help menu or . In the Protection and Provisioning dashboards, there is an additional Help icon available at the top of each dashboard panel that brings up a Help page with information about the panel.



# Dashboard panel descriptions

---

The dashboard panels provide cumulative at-a-glance status information for your system.

Dashboards are provided for each application available in NetApp Management Console .

- *Protection dashboard* on page 689 : These dashboard panels provide status on datasets, resource pools, protected data, and unprotected data.
- *Provisioning dashboard* on page 690 : These dashboard panels provide space management information related to datasets and resource pools.
- *Performance Advisor dashboard* on page 690 : These dashboard panels provide information on performance.

You can filter the content of some of the protection and provisioning dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools. When you select a group filter, only relationships originating or terminating at an object in the selected group are listed.

You must be assigned the appropriate privileges to view the dashboard panels.

## Protection dashboard

You can view more information about each dashboard panel and its contents by clicking  in the dashboard panel title bar to access the Help page for that panel.

<b>Failover Readiness</b>	Visible only when the disaster recovery option is licensed.  Displays the number of datasets configured for disaster recovery protection and that are in the failover ready state. This indicates that the datasets can successfully carry out failover operations, should failover operations become necessary.
<b>Failover Status</b>	Visible only when the disaster recovery option is licensed.  This panel appears when a failover operation is invoked, listing the number of datasets in the process of failing over and the number of datasets that have successfully failed over.
<b>Top Five Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events.
<b>Dataset Protection Status</b>	Displays the total number of protected datasets, grouped according to their current protection status value.
<b>Protected Data</b>	Displays the total number of datasets, volumes, qtrees, and Open Systems SnapVault directories that are covered by data protection policies.

<b>Unprotected Data</b>	Displays the total number of datasets, volumes, and qtrees that are not covered by data protection policies.
<b>Dataset Lags</b>	Displays any datasets that have a protection component that is out of date with the primary data. This panel groups relationships according to dataset, sorts relationships according to lag, selects the longest lag for each dataset, and displays the datasets in decreasing order of lag.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to and the space utilization for each resource pool. Items are sorted in increasing order of available space.

## Provisioning dashboard

You can view more information about each dashboard panel and its contents by clicking  in the task bar to access the Help page for that panel.

<b>Dataset Conformance Status</b>	Displays the total number of datasets that are conforming to associated policies.
<b>Top Five Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events.
<b>Dataset Resource Status</b>	Displays the number of datasets at different levels of resource status severity. The status represents the worst event severity on all direct and indirect members of the dataset nodes.
<b>Dataset Space Status</b>	Displays the total number of datasets being managed by NetApp Management Console , grouped according to their current space status value. The status represents the worst space status of all members in all nodes of the dataset. Events are generated at the dataset level when the space status of a dataset changes.
<b>Resource Pool Space Status</b>	Displays the total number of resource pools that currently meet or exceed the space thresholds.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to and the space utilization for each resource pool. Items are sorted in increasing order of available space.

## Performance Advisor dashboard

You can view more details about the Performance Advisor dashboard by clicking  in the task bar to access the dashboard Help page.

<b>Top Performance Events</b>	Displays the five events with the highest severity levels. Items are ordered first by severity, then by time of the events. More detail about each event is provided in <b>Monitor &gt; Events</b> .
-------------------------------	--

<b>Top Storage Systems by Network Throughput</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest network throughput. The number above each bar chart displays the exact value of the throughput per second from that system. The vertical axis displays the megabytes of throughput per second. The horizontal axis displays the name of the storage system .
<b>Top Storage Systems by Total OPs</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest total operations. The vertical axis displays the total operations per second for that storage system . The horizontal axis displays the storage system name.
<b>Top Storage Systems by CPU Utilization</b>	Displays a bar chart of the top five DataFabric Manager storage systems , sorted by the highest average CPU utilization. The number above each bar chart displays the exact value of the throughput per second from that system. The vertical axis displays the percentage CPU usage of the storage system . The horizontal axis displays the name of the storage system .



# Dataset concepts

---

You can use datasets to group data and use resource pools to group storage to simplify the monitoring, provisioning, reporting, and access control of your SnapVault and SnapMirror relationships, which enables flexible and efficient use of storage.

Associating a data protection, disaster recovery, or provisioning policy with a dataset lets storage administrators automate tasks, such as assigning consistent policies to primary data, propagating policy changes, and provisioning new volumes, qtrees, or LUNS on primary and secondary dataset nodes. The licenses that you have installed determine which policies are available.

Configuring a dataset combines the following objects:

<b>Dataset</b>	For protection purposes, a dataset is a collection of physical resources on a primary node, such as volumes, flexible volumes, and qtrees, and copies of backed-up data.  <b>Note:</b> It is a good practice to group primary data that have identical data protection requirements.
	For provisioning purposes, a dataset is a collection of physical resources, such as volumes, flexible volumes, qtrees, and LUNs, that are assigned to a dataset node. If the protection license is installed and the protection policy establishes a primary and one or more nonprimary nodes, each node of the dataset is a collection of physical resources that might or might not be provisioned from the same resource pool.
	A dataset cannot contain a storage system that is also in a resource pool assigned to a dataset node. This constraint prevents a loop that attempts to provision an infinite number of volumes.
<b>Application dataset</b>	A dataset managed by an application that is external to the licensed protection and provisioning applications, such as a dataset managed by SnapManager for Oracle.
<b>Resource pool</b>	A collection of physical resources from which secondary storage is provisioned. Resource pools can be used to group storage systems and aggregates by attributes, such as performance, cost, physical location, or availability.
<b>Data protection policy</b>	A data protection policy defines how to protect the primary, secondary, and tertiary storage, as well as when to create copies of data and how many copies to keep.
<b>Provisioning policy</b>	A provisioning policy defines how to provision primary or secondary dataset nodes, and provides rules for monitoring and managing storage space and for allocating storage space from available resource pools.

## Related concepts

[Overview of resource pools](#) on page 819

*What a policy is* on page 847

*What groups are* on page 1047

## How the protection application uses datasets

---

The licensed protection application uses the information in a dataset to create Snapshot copies used for backups and mirror copies, to provision storage as needed for the copies, and to transfer the copies to backup or mirror nodes.

After you set up a dataset for protection, the licensed protection application performs the following operations:

1. The application provisions volumes and qtrees on the destination node in several ways. For storage systems that run Data ONTAP 7.0 or later, the application automatically provisions flexible volumes and qtrees when the resource pool contains an aggregate. For storage systems that run Data ONTAP 6.5 or earlier, you manually add secondary storage to the destination node. If you manually select storage without using resource pools for a SnapMirror destination node, the application provisions traditional volumes assigned to that destination node.
2. The application creates backup relationships (either SnapVault or SnapMirror) between volumes and qtrees in the dataset with the newly provisioned secondary storage.
3. The application runs the data protection schedules, making Snapshot copies of the primary data and initiating SnapVault and SnapMirror baseline transfers at the scheduled times.
4. The application periodically checks that the dataset conforms to its data protection policy. If either the dataset membership or the policy changes, the application tries to bring the dataset back into conformance, or it notifies you that the conformance status changed to nonconformant.



# How the provisioning application works with datasets

---

The licensed provisioning application simplifies and automates the tasks of provisioning and managing storage for the data in datasets.

After you add a dataset for provisioning, the licensed provisioning application performs the following operations:

- Provisions the dataset

The application provisions volumes and qtrees (in NAS environments) or volumes and LUNs (in SAN environments) for a dataset using the resource pool assigned to the dataset. In SAN environments, a provisioned volume can be delegated to SDx applications and used to create qtrees or LUNs.

If you have the provisioning license only, the primary dataset node is provisioned.

If you also have the protection license, the licensed provisioning application can provision volumes, qtrees, or LUNs on the backup and mirror dataset nodes.

**Note:** You are advised NOT to use SnapDrive for Windows versions lower than 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error requiring the LUNs to be manually unmapped.

- Configures automatic storage using policies and templates

When you create a dataset for provisioning, you can assign a provisioning policy that provides settings for automatically configuring storage for the dataset.

- Allows manual addition of storage space

You can manually add additional volumes, qtrees, or LUNs, at any time, to a dataset that has a provisioning policy assigned.

- Handles dataset-managed protocols for exporting data

Protocols for exporting data are automatically handled by the dataset.

You can also assign a vFiler template to a vFiler host. When a vFiler host is created, the vFiler template provides default settings for automatically configuring the vFiler host.

- Checks for conformance

The application periodically checks that the dataset conforms to its provisioning policy. For example, if the data in a dataset reaches a specified threshold level, the application tries to create additional space according to the provisioning policy, either by increasing the storage container size or deleting old Snapshot copies, or both. If it cannot bring the dataset back into conformance, it notifies you that the conformance status changed to nonconformant.

- Allows manual management of storage space

The application provides manual controls for viewing and resizing individual volumes or qtrees and modifying volume data and Snapshot copy space allocations.



# About NFS, CIFS, iSCSI, or FC protocol access

---

You can configure NFS, CIFS, iSCSI, or Fibre Channel (FC) export protocols for client access to a dataset.

You can specify support for export protocol access when you create a dataset, when you reconfigure the primary, backup, or mirror nodes in your dataset, or when you provision a new volume, LUN, or qtree into the dataset.

There are two ways that you can export storage in a dataset.

You can enable one export protocol for an entire primary, backup, or mirror node of a dataset. Clients can access all of the storage, that is all volumes, qtrees, and LUNs, in a particular dataset node by using the specified protocol.

To achieve this configuration, specify export settings for the primary node when completing the **Add Dataset** wizard and for the backup and mirror nodes by using the **Dataset Policy Change** wizard.

You can assign different export protocols to each new volume, LUN, or qtree member when you provision the member into a dataset, rather than specifying an export protocol for the entire dataset node. Clients can selectively access dataset members, based on the protocols enabled for each client and each dataset member.

To achieve this configuration, do not specify an export protocol when creating a dataset. Instead, use the **Provisioning** wizard to provision a new member into a dataset and select the option to export the new member.

**Note:** The export settings presented in the **Provisioning** wizard are determined by the provisioning policy type assigned to the dataset.

## Related concepts

[Overview of export protocol properties](#) on page 743

## Related tasks

[Configuring dataset nodes for NFS protocol access](#) on page 747

[Configuring dataset nodes for CIFS protocol access](#) on page 745

[Configuring dataset nodes for FC protocol access](#) on page 749

[Configuring dataset nodes for iSCSI protocol access](#) on page 751



# When to configure datasets

---

You should configure datasets when you have identified which data to group for protection or provisioning.

You can also configure datasets in the following situations:

## Protection

- You installed the protection license and are setting up data protection for the first time.
- You previously used Backup Manager or Disaster Recovery Manager and are upgrading to the licensed protection application, and you want to import existing relationships that the licensed application discovered.
- You never used Operations Manager to monitor or manage your SnapVault or SnapMirror relationships and want to import existing relationships that the licensed protection application discovered.
- A condition changed that affects the status of the dataset, and you want to change the protection policy.
- You are monitoring your storage resources by viewing the dashboard, which displays resources as well as which resources are unprotected.
- You added a storage system, or DataFabric Manager discovered it, and you want to protect the data on that storage system.

## Provisioning

- You installed the provisioning license and are setting up provisioning for the first time.
- You want to provision an existing dataset that has not yet been provisioned.
- You need to add another volume or LUN to an existing dataset.
- A condition changed that affects the status of the dataset, and you want to change the provisioning policy.
- You are monitoring your storage space usage by viewing the dashboard and it displays a warning for a dataset member that is running out of space.



## How to enable backup of multiple primary volumes to a single secondary volume

---

You can configure your protection application to support SnapVault-based or Qtree SnapMirror-based backup of multiple volumes in primary storage to a single volume in secondary storage.

By default, the protection application automatically sets up one-to-one backup relationships between primary and secondary volumes when provisioning secondary nodes in datasets. But in circumstances in which the 500-volume limit for storage systems might not allow a one-to-one ratio of primary volumes to secondary volumes, you can configure the protection application through the Operations Manager global option `dpMaxFanInRatio` (to support backup relationships between multiple volumes in primary storage and a single volume in secondary storage).

**Note:** The following limitations apply to protection application support for automatically configuring backup relationships of multiple primary volumes to a single secondary volume when provisioning secondary storage:

- The protection application does not support volume SnapMirror-based mirroring from multiple primary volumes to a single secondary volume.
- All the primary volumes and the secondary volume must be members of the same dataset.
- The protection application implementation of Open Systems SnapVault backup is not affected by the `dpMaxFanInRatio` option.

For more information on the `dpMaxFanInRatio` global option, see the Operations Manager online Help.



# **Dataset storage space management**

---

The licensed provisioning application enables you to view space allocations for volumes, LUNs, and qtrees. You can also resize individual volumes or qtrees, and modify volume data and Snapshot copy space allocations in response to space-usage generated error or warning events.

The space allocation changes that you make apply only to the selected volume or qtree, not to any other volumes or qtrees in the dataset. You can specifically edit the space allocation for data and Snapshot copies as long as the space allocation remains compliant with the provisioning policy assigned to the associated dataset primary, backup, or mirror node.

## **Next topics**

[\*When to manually manage storage space for a dataset\*](#) on page 705

[\*How to view dataset storage space utilization\*](#) on page 706

[\*Overview of tasks for managing storage space\*](#) on page 706

[\*Space management resize options\*](#) on page 707

## **Related tasks**

[\*Viewing volume, LUN or qtree space allocation\*](#) on page 757

[\*Diagnosing volume or qtree space status\*](#) on page 759

[\*Resizing volume space\*](#) on page 761

[\*Resizing qtree space\*](#) on page 763

[\*Deleting Snapshot copies\*](#) on page 765

[\*Deleting a volume, LUN or qtree\*](#) on page 767

## **When to manually manage storage space for a dataset**

In most cases, you perform space management tasks on a volume, or qtree when a space-usage generated warning or error event alerts you to the fact that an individual storage container in one of your managed datasets has reached, or is close to reaching, its configured maximum capacity to hold new data.

At this point, in many cases, the simplest and most immediate remedy is to make more data space available for those individual volumes or qtrees.

**Note:** The only management task that you can perform on a LUN is to delete the LUN.

## How to view dataset storage space utilization

You can use the **Resource Pools** window Space breakout tab to see how much space each dataset is currently using, which is helpful for determining when a dataset needs to be migrated to a larger aggregate in another storage system.

The Space breakout tab lists the aggregates assigned to the resource pool that is selected in the **Resource Pools** window. When you select an aggregate, all the datasets in the aggregate and the percentage and amount of currently used space for each dataset are displayed.

Datasets that have a high percentage of utilization are good candidates for migration.

## Overview of tasks for managing storage space

If you have the provisioning license, you can perform different tasks to manage the storage space for a dataset.

### **Survey your volumes and qtrees.**

You can scan the tables on the Provisioning tab to pinpoint the volumes and qtrees that are approaching their data and Snapshot copy space limitation.

### **Diagnose your space management warning and error statuses.**

You can check the diagnosis of the volumes or qtrees whose space status is Warning or Error.

### **Resize your volume or qtree data and Snapshot space.**

In nodes containing volumes or qtrees, you can expand a volume to claim more uncommitted aggregate space or you can increase a qtree quota to claim more uncommitted volume space. You can also reallocate the space in a volume specifically reserved for Snapshot copies and specifically used for data.

### **Delete Snapshot copies.**

You can delete individual Snapshot copies in a volume to make more space available for data.

### **Delete storage containers.**

You can delete unneeded volumes and return the space that they used to the containing aggregate for reallocation. You can delete LUNs and qtrees and return the space they used to the containing volume for reallocation.

## Space management resize options

The provisioning application allows you as many as three options to resize or reallocate space on existing volumes. It also allows you to expand hard quotas on existing qtrees.

<b>Volume resize options</b>	Depending on the type of volume (NAS or SAN), the provisioning application enables you to modify one or more of the following parameters:
<b>Total volume size</b>	You can increase the total space allowed for the selected NAS or SAN volume within its containing aggregate. If you are not allowing space overcommitment, you are limited by the amount of space still available in the containing aggregate.
<b>Snap reserve %</b>	The percentage of space in the selected flexible volumes reserved for Snapshot copies. Snap reserve % is adjustable on NAS volumes. As you adjust the percentage up or down, the provisioning application displays the absolute allocation of Snapshot copy reserve space in the Snap Reserve field.
<b>Maximum size limit</b>	If the Autogrow property is enabled on a SAN or NAS volume, you can modify the Maximum size limit.

<b>Qtree resize option</b>	The provisioning application allows you to enlarge the hard quota for a qtree if the qtree is configured with a hard quota.
----------------------------	---

### Related tasks

[Resizing volume space](#) on page 761



# Dataset properties

---

You can use the following definitions when you configure or edit a dataset's properties and resources.

## General properties

The dataset properties menu enables you to modify the name, description, custom name prefix, ownership, and policy enforcement properties of an existing dataset. For an application dataset, the name of the application that created the dataset, the application version, and the server name running the application, also appear.

<b>Name</b>	The name of the dataset
<b>Description</b>	The description of the dataset
<b>Volume and qtree name prefix</b>	The prefix used to designate the volume or qtree in a dataset. The name prefix defaults to the dataset name or you can specify a custom prefix.
<b>Owner</b>	The name of the person responsible for this dataset
<b>Contact</b>	The e-mail address of each person who should be contacted about this dataset. You can separate multiple e-mail addresses with commas.
<b>Time Zone</b>	The time zone that protection policy schedules should use when timing protection events.
<b>IP address and netmask</b>	The IP address and netmask of the vFiler unit that will be provisioned when the first member of the dataset is provisioned. This property is active only for datasets that do not have a vFiler unit assigned.

## Related concepts

[Decisions to make before adding datasets](#) on page 711

## Related tasks

[Adding a dataset](#) on page 719



# Decisions to make before adding datasets

---

Before you use the **Add Dataset** wizard to create a dataset, you need to decide how you want to protect and provision the dataset.

## Next topics

*[Dataset protection decisions](#)* on page 711

*[Dataset provisioning decisions](#)* on page 714

*[Custom name prefixes for dataset volumes, qtrees, and Snapshot copies](#)* on page 716

## Related concepts

*[Effect of time zones on schedules](#)* on page 1049

*[What a protection policy is](#)* on page 847

*[Overview of resource pools](#)* on page 819

*[Protection policy node prerequisites](#)* on page 1051

*[What a provisioning policy is](#)* on page 848

## Related tasks

*[Adding a dataset](#)* on page 719

## Related references

*[Dataset properties](#)* on page 709

# Dataset protection decisions

Before you use the **Add Dataset** wizard to create a new dataset, and if you have the protection license, you need to decide how you want to protect the data and how you want to assign resources to contain backups or mirror copies.

**Dataset properties**

- When naming the dataset, is there a naming convention at your site to help administrators locate and identify datasets?

Dataset names can include the following characters:

a to z  
A to Z  
0 to 9  
. (period)  
\_ (underscore)  
- (hyphen)  
space

If you use any other characters when naming the dataset, they will not appear in the name.

- What is a good description of the dataset membership?

Use a description so that someone unfamiliar with the dataset and the reasons supporting its creation understand its purpose.

- Will you include a volume and qtree name prefix so you can easily find all volumes and qtrees associated with the dataset?

Volume and qtree name prefixes can include the following characters:

a to z  
A to Z  
0 to 9  
. (period)  
\_ (underscore)

If you use any other characters, you will get an error message.

If you do not use a volume and qtree name prefix, the dataset name will be used.

- Who is the owner of the dataset?
- If an event on the dataset triggers an alarm, who should be contacted?  
You can provide an individual e-mail address for each person or a distribution list of people to be contacted.
- Should operations on the dataset be scheduled according to the local time zone for the data?

If so, you can specify a time zone in the wizard or use the default time zone, which is the system time zone used by the DataFabric Manager server.

- |                          |  |
|--------------------------|--|
| <b>Group membership</b>  | <ul style="list-style-type: none"> <li>• Do you need to create a collection of datasets and resource pools based on common characteristics, such as location, project, or owning organization?</li> <li>• Is there an existing group to which you want to add this dataset?</li> </ul>   |
| <b>Protection policy</b> | <ul style="list-style-type: none"> <li>• Which protection policy meets the requirements of the dataset?<br/>Review the policies listed on the <b>Protection Policies</b> window to see if any are suitable for your new dataset.</li> <li>• If no protection policy meets the requirements of your new dataset, is there a protection policy that would be suitable with minor modifications?<br/>If so, you can copy that protection policy to create a new policy you can modify as needed for the new dataset. If not, you can run the <b>Add Protection Policy</b> wizard to create a new policy for the dataset.</li> </ul> <p><b>Note:</b> You do not have to assign a policy to create a new dataset. You can assign a policy to the dataset later by running the <b>Dataset Policy Change</b> wizard.</p>  |
| <b>Resources</b>         | <p>Will you assign a resource pool or individual physical resources as destinations for your backups and mirror copies?</p> <p>You do not have to assign a resource pool or physical resources to a node to create a new dataset. However, the dataset will be nonconformant with its policy until resources are assigned to each node, because the licensed protection application cannot carry out the protection specified by the policy.</p> <p>If using a resource pool:</p> <ul style="list-style-type: none"> <li>• For each node in the dataset, which resource pool meets its provisioning requirements?<br/>For example, the resource pool you assign to a mirror node should contain physical resources that would all be acceptable destinations for mirror copies created of the dataset members.</li> <li>• If no resource pool meets the requirements of a node, you can create a new resource pool for each node at the <b>Resource Pools</b> window.</li> <li>• Verify that you have the appropriate software licenses on the storage you intend to use.</li> </ul> <p>If using individual resources:</p> <ul style="list-style-type: none"> <li>• If you prefer not to use resource pools for automatic provisioning, you can select individual physical resources as destinations for backups and mirror copies of your dataset.</li> <li>• Verify that you have the appropriate software licenses on the storage you intend to use.</li> </ul> |

## Related concepts

[What a protection policy is](#) on page 847

[Effect of time zones on schedules](#) on page 1049

[What a provisioning policy is](#) on page 848

## Dataset provisioning decisions

If you have the provisioning license, you must gather certain provisioning information before you use the **Add Dataset** wizard to create a new dataset. A dataset can have a single node or, if you assign a protection policy to it, a dataset can have a primary and one or more nonprimary nodes. When you first create a dataset, you configure the provisioning for the primary node only.

**Provisioning policy for** Do you want to assign a provisioning policy to manage the storage resources or do you want to manually assign resources?

**primary node**

- If you want to use a provisioning policy, have you already configured a policy that meets the requirements of the data in the dataset primary node? Review any existing policies that are listed in the **Provisioning Policies** window to see if any are suitable for your new dataset.
- If no current provisioning policy meets the requirements of your new dataset, is there a policy that would be suitable with minor modifications? If so, you can copy that policy and then modify it as needed. If no suitable provisioning policy exists, you can run the **Add Provisioning Policy** wizard to create a new policy.
- If you do not want to assign a provisioning policy at the time the dataset is created, you can assign a provisioning policy to the primary node later.

**Note:** After the dataset is added, whether or not it has a provisioning policy assigned, you can also provision new members for the dataset by using the **Provisioning** wizard.

- If you assign a NAS-based provisioning policy, do you want to enable CIFS or NFS export protocol access to the members of this dataset node?

You can enable one or both export protocols for all members of this node when you configure the dataset. You can also decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

However, you cannot enable CIFS export protocol access if the assigned provisioning policy is configured for the options "Guarantee space for dataset and Snapshot copies" (which is displayed in the **Provisioning Policies** window as "Guarantee space for dataset") and ""Guarantee initial size, allocate maximum size on-demand and allow automatic deletion of Snapshot copies" (which is displayed in the **Provisioning Policies** window as "Increase container size automatically").

- If you assign a SAN-based provisioning policy, do you want to enable FC or iSCSI export protocol access to the members of this dataset node?  
You can enable either protocol for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

<b>vFiler unit assignment and data migration capability</b>	<p>Do you want to attach a vFiler unit to the dataset for data export?</p> <p>If so, you can select an existing vFiler unit that is managed by the provisioning application or you can provide an IP address or network mask and the provisioning application will create a new vFiler unit. Attaching a vFiler unit enables automatic offline migration for the dataset. (Automatic offline migration requires that you shut down applications using the dataset before initiating the cutover step of the migration process.)</p>
<b>Nonprimary dataset nodes</b>	<p>After the dataset is created, if you have the protection license and the dataset has a secondary backup or mirror node, you can edit the dataset node to assign a provisioning policy to a nonprimary node.</p> <ul style="list-style-type: none"> <li>• If you choose to associate a vFiler unit with a nonprimary node in a dataset, any volumes that are provisioned for that dataset must be associated with the vFiler unit. Therefore, when you view a list of the dataset volumes, only volumes that are owned by the vFiler unit are displayed.</li> </ul>

**Note:** You cannot associate a vFiler unit with a nonprimary node unless it is a disaster recovery-capable nonprimary node.

- If you want to assign a NAS or SAN type provisioning policy instead of a secondary type policy to a nonprimary node, the dataset must be disaster recovery capable. This means that the dataset must also have a protection policy assigned that supports disaster recovery, and the nonprimary node must be the disaster recovery-capable node.
- The policy type (NAS or SAN) on the primary dataset node must match the policy type assigned to the nonprimary node.
- If you assign a NAS-based provisioning policy, do you want to enable CIFS or NFS export protocol access to the members of this dataset node?  
You can enable one or both export protocols for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.
- If you assign a SAN-based provisioning policy, do you want to enable FC or iSCSI export protocol access to the members of this dataset node?  
You can enable either export protocol for all members of this node when you configure the dataset, or, alternatively, you can decline to enable export protocols

at the dataset node level and later enable export protocols for individual members as you provision them into this dataset.

**Note:** You should not use a version earlier than SnapDrive for Windows 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error, after which you must manually unmap the LUNs.

#### Related concepts

[Dataset migration overview](#) on page 769

[Overview of export protocol properties](#) on page 743

[What a provisioning policy is](#) on page 848

#### Related references

[Dataset migration requirements](#) on page 771

## Custom name prefixes for dataset volumes, qtrees, and Snapshot copies

When creating or editing a dataset, you can choose a custom name prefix for the volumes and qtrees in the dataset, and for the Snapshot copies. The name prefix helps you to easily locate volumes, qtrees, and Snapshot copies.

**Naming for primary nodes** For NAS provisioned datasets, you can specify a custom volume and qtree name prefix for all volumes included within the dataset. You can name the qtrees within those volumes at the time you create the qtree. If you do not use a volume and qtree name prefix, the dataset name is used.

The volume and qtree name prefix can include the following characters:

- a to z
- A to Z
- 0 to 9
- . (period)
- \_ (underscore)
- (hyphen)
- space

If you use other characters, you get an error message.

The volume and qtree name prefix is the volume name. Volume names are limited to 64 total characters, including underscores and suffixes. Suffixes are added if the volume name is a duplicate.

**Naming for nonprimary nodes**

For nonprimary nodes, you can specify a volume and qtree name prefix to apply to backups and mirrored copies. If your primary node is unavailable, you can locate the appropriate volumes and qtrees on a nonprimary node, using the naming prefix you specified when you created or edited your dataset.

The backup name consists of the volume and qtree name prefix and the backup type. Root qtrees being backed up on nonprimary nodes use the volume and qtree name prefix. However, qtrees created before the release of DataFabric Manager 3.8 will not use the volume and qtree name prefix.

The name of the mirrored copy includes the secondary volume and qtree name prefix, mirror type, primary host name, and the primary volume name.

For nodes that use the backup then mirror policy, the name includes the volume and qtree name prefix and the backup type (mirror).

If you do not specify a volume and qtree name prefix, the dataset name will be used.

For more information on the CLI commands necessary to access the nonprimary node, see the DataFabric Manager man pages.

**Naming Snapshot copies**

Snapshot copies have a date stamp prefix. The full name also includes the retention type, host name, volume name, and the qtrees included within the Snapshot copy. The name is shortened if there are too many qtrees in the Snapshot copy.

For more information on CLI commands for Snapshot copy naming, see the DataFabric Manager man pages.



# Adding a dataset

---

You can add a dataset to manage protection for data sharing the same protection requirements, or to manage provisioning for the dataset members.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
  - Provisioning policy for nonprimary dataset nodes
- If you plan to assign a policy, you need to be assigned a role that enables you to view policies.
- If you plan to assign a provisioning policy, you also need a role that enables you to attach the resource pools configured for the policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Datasets ▶ Overview**.
2. Click **Add** to start the **Add Dataset** wizard.

If you want to provision your node by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.

**Note:** If you receive a message that the maximum number of vFiler units has been reached, you must relinquish the migration capability for one or more datasets before you can configure an IP address and network mask that enables the migration capability for a dataset.

3. Complete the steps in the wizard to create a dataset.

If you have the protection license and you did not assign a protection policy to the dataset or assign resources to each destination node when creating the new dataset, the data is not yet protected.

If you have the provisioning license and you did not assign a provisioning policy to each of the dataset nodes, you will have to manually provision each node.

If you have the disaster recovery license and you did not assign a disaster recovery policy to the dataset, the data is not protected for disaster recovery.

### **Related concepts**

*[Decisions to make before adding datasets](#)* on page 711

*[Effect of time zones on schedules](#)* on page 1049

*[Decisions to make before adding datasets](#)* on page 711

### **Related tasks**

*[Relinquishing migration capability of a dataset](#)* on page 797

*[How do I back up data?](#)* on page 589

*[Enabling disaster recovery protection](#)* on page 641

### **Related references**

*[Dataset properties](#)* on page 709

*[Administrator roles and capabilities](#)* on page 1055

# Decisions to make before assigning or changing policies

---

Before you assign or change a policy, you need to gather information about the dataset and policies that you want the dataset to have.

You will need to gather the following information:

## Protection policy

- Which protection policy meets the requirements of the dataset?  
Review the policies listed on the **Protection Policies** window to see if any is suitable for your new dataset.
- If no protection policy meets the requirements of your new dataset, is there a protection policy that would be suitable with minor modifications?  
If so, you can copy that protection policy to create a new policy you can modify as needed for the new dataset. If no suitable protection policy exists, you can run the **Add Protection Policy** wizard to create a new policy for the dataset.

## Disaster recovery policy

- What type of disaster recovery capable protection policy do you need?  
The licensed protection application provides disaster recovery capable protection policies that function similarly to the backup policies.

**Note:** When you change a policy from backup to mirror or mirror to backup, the **Dataset Policy Change** wizard prompts you to establish a new baseline for the relationship. If you do, old data is retained, and the application makes a new copy of the entire dataset and transfers the active file system on the secondary. After reinitialization, you can manually delete the Snapshot copy.

- If you are changing the protection policy to a disaster recovery policy, do you want to map the settings from a node in the old dataset to a node in the new dataset?  
You should copy the settings only if the path from the primary node is the same in the new policy as it was in the old policy.
- Do you plan to use a failover script to shut down processes before the application invokes failover?  
If so, you need to define the path to a failover script.

## Backup and mirror node resources

- If you are changing the protection policy for a dataset with backup and mirror nodes, do you want to use the same resource assignments that were used in the previous policy?  
For example, if you have a dataset using the Mirror policy and you want to change to the Chain of two mirrors policy, you can choose to copy resources used for the single mirror node in the current policy to one of the two mirror nodes in the new

policy. After you have copied resources from a node in the current policy, you cannot copy resources from that same node to any other node in the new policy.

- If you are assigning a policy for the first time or if you do not want to copy resources used in the current policy, is there a resource pool that meets the provisioning requirements of the dataset?

For example, the resource pool you assign to a mirror node should contain physical resources that would all be acceptable destinations for mirror copies created of the dataset members. If no resource pool meets the requirements of a nonprimary node, you can create a new resource pool for each backup and mirror node using the **Add Resource Pool** wizard.

- If you prefer to not use resource pools for automatic provisioning, which physical resources would be suitable as destinations for backups and mirror copies of the dataset?

**Note:** You do not have to assign a resource pool or physical resources to a destination node to assign or change a policy. However, the dataset will be nonconformant with its new policy until resources are assigned to each destination node, because the licensed application cannot carry out the protection specified by the policy.

#### Provisioning policy

- On which node do you want to assign or change the provisioning policy? If you have a protection license, your dataset might have a primary and one or more nonprimary nodes. You can assign the same provisioning policy to every node in the dataset, or you can assign a different provisioning policy to each node.
- Which provisioning policy meets the requirements of the dataset node? Review the policies listed on the **Provisioning Policies** window to see if any is suitable for the dataset node.

**Note:** If you are changing the provisioning policy, the policy type (NAS or SAN) on the primary dataset node must match the policy type assigned to the nonprimary node. If you want to assign a NAS or SAN type provisioning policy instead of a secondary type policy to a nonprimary node, the dataset must be disaster recovery capable. This means that it must also have a protection policy assigned that supports disaster recovery, and the node must be the disaster recovery capable node.

- If no provisioning policy meets the requirements of the dataset node, is there a provisioning policy that would be suitable with minor modifications? If so, you can copy that policy to create a new policy that you can modify as needed. If not, you can run the **Add Provisioning Policy** wizard to create a new policy for the dataset node.

#### Related concepts

[What a protection policy is](#) on page 847

*[Overview of resource pools](#)* on page 819

**Related tasks**

*[Assigning or changing a protection policy](#)* on page 725



# Assigning or changing a protection policy

---

You can assign a policy to a dataset or change the policy assigned to it. The policy specifies how the data is to be protected.

## Before you begin

- Have the protection information available that you need to complete this task:
  - Dataset properties
  - Group membership
  - Protection policy
- Determine which policy you want to assign to the dataset. You can review available protection policies on the **Protection Policies** window. If no policy meets the requirements of your new dataset, you can create a new policy or modify a copy of an existing policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can use this procedure after you have created a new dataset and want to assign a policy to it, or when you want to change the protection policy assigned to a dataset. You can also use this procedure to protect a dataset that is listed on the **Datasets** window.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select a dataset and click **Protection Policy** to start the **Dataset Policy Change** wizard.

**Note:** If you want to provision your nodes by resource pool, click the **Use provisioning policy** option when it is displayed, even if you do not have the provisioning application licensed.

3. Complete the steps in the wizard.

## Related concepts

[\*Decisions to make before assigning or changing policies\*](#) on page 721

[\*What a protection policy is\*](#) on page 847

**Related tasks**

*How do I back up data?* on page 589

*Enabling disaster recovery protection* on page 641

**Related references**

*Administrator roles and capabilities* on page 1055

# Assigning or changing a provisioning policy

---

You can assign a provisioning policy to a dataset node or change the currently assigned provisioning policy assigned to a dataset node.

## Before you begin

- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
  - Provisioning policy for nonprimary dataset nodes
- Determine which policy you want to assign to the dataset node. You can review available provisioning policies listed in the **Provisioning Policies** window.  
If no provisioning policy meets the requirements of your dataset node, you can create and modify a copy of an existing policy or create a new policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to assign or change the provisioning policy and click **Edit**.
3. In the **Edit Dataset** window, click **Provisioning/Resource Pools** for the node to which you want to assign or change the provisioning policy.
4. On the Edit Provisioning and Resource Pools page, select a provisioning policy and click **Next**.
5. Continue to click **Next** until you reach the Preview Details page.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.
7. Close the **Edit Dataset** window.

## Related tasks

[Enabling deduplication on your dataset nodes](#) on page 809

## Related references

[Administrator roles and capabilities](#) on page 1055



# Decisions to make before provisioning a dataset

---

Before you use the **Provisioning** wizard to add a volume, qtree, or LUN to an existing primary dataset node, you need to gather the information required to complete the wizard.

**Prerequisites** Does the dataset that you are trying to provision have a resource pool assigned to it?

If not, you need to assign a resource pool before provisioning the node. You can check the resource pool assignment on the **Datasets** window Overview tab.

Does the dataset that you are trying to provision have a provisioning policy assigned to it?

If not, you need to assign a provisioning policy before provisioning the node. You can check the provisioning policy assignment on the **Datasets** window Overview tab.

**Note:** You are advised not to use SnapDrive for Windows versions earlier than 5.0 to connect to mapped LUNs that are provisioned through the licensed provisioning management application. Doing so might result in an error that requires the LUNs to be manually unmapped.

**Name** What is the export name of the volume or LUN that you want to provision?

The export name (NFS or CIFS protocol for NAS storage, or iSCSI or FCP protocol for SAN storage) is created with the name you specify.

**Description** What is the description of this provisioning request?

This information can be useful later: for example, if you want to track provisioning requests against IT helpdesk tickets.

**Size** What is the size of the qtree, volume or LUN?

- The minimum LUN size for Windows is 32 MB. For other operating systems it is 4 MB.
- The actual size that is provisioned is determined by the size that you specify in the wizard and by the provisioning policy that is assigned to the dataset node.
- **NAS storage example**

If you enter a maximum size of 20 GB in the wizard and the provisioning policy that is assigned to the dataset enables the Reserve space for Snapshot copies option, then the licensed application allocates 24 GB for the newly provisioned storage. If the provisioning policy does not enable the option for guaranteed space for data and Snapshot copies, the licensed application does not allocate space until the space is actually used. In this case, the total size refers only to the potential size that can be used, but the space is not guaranteed.

- SAN storage example

If you enter 50 GB for the data size and 50 GB for the maximum Snapshot copy size, and if the provisioning policy that is assigned to the dataset enables the option to guarantee space for data and Snapshot copies, the licensed application adds 50 GB for the overwrite reserve space and allocates a total of 150 GB for the volume.

What is the maximum space for Snapshot copies?

- If you are provisioning a LUN, what is the maximum amount of space in the volume that Snapshot copies can use?
- If you are provisioning a volume or qtree, what is the maximum amount of space in the resource pool that the volume or qtree can use?

When calculating the amount, include all of the LUNs, space reserves, and Snapshot copy space that the resource pool contains.

**Override exports** Which, if any, export protocol access do you want to enable for the volume, LUN, or qtree that you are provisioning?

This decision applies only if you have not already enabled an export protocol on the entire dataset into which you are provisioning the volume, LUN, or qtree.

- If you are provisioning NAS storage, do you want to enable NFS export access, CIFS export access, or both?
- If you are provisioning SAN storage, do you want to enable iSCSI export access or FC export access?

**Resource selection** How do you want to select the resource to provision into this dataset?

- Do you want the provisioning application to automatically provision a resource from the assigned resource pool?
- Do you want to manually select the resource from the assigned resource pool?

## Related concepts

[Overview of export protocol properties](#) on page 743

[How to select a specific aggregate or storage system for provisioning](#) on page 733

## Related tasks

[Provisioning resources for a primary dataset node](#) on page 731

# Provisioning resources for a primary dataset node

You can add a volume to the primary dataset node when you need to add more space to an existing dataset.

## Before you begin

- Have the provisioning information available that you need to complete this task:
  - Provisioning policy for primary node
  - Migration capability
  - vFiler unit assignment
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Provisioning**.
2. Select the dataset that you want to provision.
3. Click **Provision** to start the **Provisioning** wizard.
4. On the Preview page, if any errors are displayed, click **Back** to return to previous pages in the wizard and correct the errors.

The Preview page displays the results of a trial run of your provisioning request. Any potential errors are described and suggestions for resolving them are provided.

5. Complete the steps in the wizard and click **Next** in the Preview page to commit the provisioning request.

The provisioning request is sent to the server. The progress of the job is shown in the progress bar. When the job completes, the **Provisioning to the dataset** summary page on the wizard confirms the completion.

If you do not want to wait for the job to complete, you can close the wizard and processing continues in the background. You can monitor the progress of the provisioning job in the **Jobs** window.

When the job is done and the new volume is added, the licensed provisioning application compares the attributes of the volume to the provisioning policy assigned to the node, if any. If the new dataset member is out of conformance, the dataset status changes to Error and the conformance status for the dataset member changes to Nonconformant.

## Related concepts

[How to select a specific aggregate or storage system for provisioning](#) on page 733

*Decisions to make before provisioning a dataset* on page 729

**Related references**

*Administrator roles and capabilities* on page 1055

# How to select a specific aggregate or storage system for provisioning

---

When using the **Provisioning** wizard to add a new volume, qtree, or LUN container in the primary node of an existing dataset, you can provision that container with a specific aggregate or storage system from its assigned resource pool rather than having the **Provisioning** wizard automatically provision aggregates or storage systems from that resource pool.

When provisioning LUNs in a SAN environment, you might need to manually select a specific storage system from resource pool if the host that you are provisioning the LUNs for has access to only that specific storage system.

To provision a new volume, qtree, or LUN with a specific aggregate or storage system, you start the **Provisioning** wizard as you normally do.

When the **Provisioning** wizard displays the "Resource selection" panel, click **Manually select a resource from the attached resource pools** and select a specific storage system or aggregate from the resource pool trees display.

## Related concepts

[\*Decisions to make before provisioning a dataset\*](#) on page 729

## Related tasks

[\*Provisioning resources for a primary dataset node\*](#) on page 731



# Decisions to make before adding or changing resource assignments

---

Before you add or change the physical resources assigned to an existing dataset node, you need to gather the required information.

- For each node in the dataset, which resource pool meets its protection or provisioning requirements? For example, if you have the protection license, the resource pool you assign to a mirror node should contain physical resources that are appropriate for mirrored copies of the dataset. If you have the provisioning license, the resource pool you assign to a dataset node should contain physical resources that are appropriate and large enough for the provisioning needs of the data contained in the dataset node.
- What if there are no resource pools that meet the protection or provisioning requirements of the dataset node? If no resource pool meets the protection or provisioning requirements of a dataset node, you can use the **Resource Pools** window to create a new resource pool for each node.
- If you have the protection and disaster recovery license, can you choose not to use resource pools? You can select physical resources for the backup and mirror nodes of your dataset. If you choose to select storage outside of a resource pool, the licensed protection application does not create volumes but instead uses the volumes you select for that dataset node.
- If you have the provisioning or disaster recovery license, can you choose not to use resource pools? You can manually provision your dataset. If you choose to provision your dataset on storage outside of a resource pool, the licensed provisioning application does not create volumes but instead uses the volumes that you select for that dataset node.

**Note:** If you choose to associate a vFiler unit with a nonprimary node in a dataset, any volumes that are provisioned for that dataset must be associated with the vFiler unit. Therefore, when you view a list of the dataset volumes, only volumes that are owned by the vFiler are displayed.

## Related tasks

[Making the disaster recovery node the new primary data storage](#) on page 649



# Adding resources to a dataset

---

You can add physical resources to an existing dataset. Any protection, disaster recovery, and provisioning policy assigned to the dataset node is automatically extended to the newly added resources.

## Before you begin

- Have the resource information available that you need to complete this task:
  - Whether or not you want to use resource pools
  - The node's protection or provisioning requirements
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to add physical resources and click **Edit**.
3. In the **Properties** sheet, click **Physical Resources** for the node to which you want to add physical resources.

The Edit property sheet Overview page is the starting point for several different types of tasks. Each option on the menu starts an in-place property sheet or a wizard. Canceling or completing an option returns you to the Edit Overview page.

4. In the Edit Physical Resources page, select each new member from the Available Resources list and move it to the Resources in this Node list.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this Dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

You can filter the list of available resources by using the Group and Resource Type drop down menus. The Group filter allows you to view data that pertains to objects in the selected group. The Resource Type filter allows you to sort by either hosts, aggregates, qtrees, or volumes. You will be able to see the resources for which you have permissions.

5. Click **Next**.

The licensed application generates a report detailing the impact of the changes to the dataset.

6. After you are satisfied with the preview results, click **Next** to apply your changes, then click **Finish** to return to the property sheet Overview page.

The licensed application updates the physical resources of the dataset.

**Related references**

*Administrator roles and capabilities* on page 1055

# Changing dataset node resource assignments

---

If the protection, failover, or provisioning requirements of your dataset change, you can add physical resources to a dataset node or change the resources currently assigned to a dataset node.

## Before you begin

- Have the resource information available that you need to complete this task:
  - Whether or not you want to use resource pools
  - The node's protection or provisioning requirements
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset to which you want to change physical resources and click **Edit**.
3. In the **Edit Dataset** window, click **Physical Resources** for the node to which you want to change the physical resources.
4. In the Edit Physical Resources page, add a new physical resource by selecting a resource from the Available Resources list and moving it to the Resources in this Node list.

Remove a resource by selecting a resource from the Resources in this Node list and moving it to the Available Resources list.

You can filter the list of available resources by using the Group and Resource Type drop down menus. The Group filter allows you to view data that pertains to objects in the selected group. The Resource Type filter allows you to sort by either hosts, aggregates, qtrees, or volumes. You will be able to see the resources for which you have permissions.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

5. Click **Next**.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.

If no resources were previously assigned to the dataset node, the dotted outline in the graph area of the **Datasets** window Overview tab is replaced by an icon representing assigned storage.

**Related concepts**

*What groups are* on page 1047

**Related references**

*Administrator roles and capabilities* on page 1055

# Removing resources from a dataset

---

You can remove physical resources from an existing dataset when you no longer want to protect, fail over, or provision its data using the assigned policy.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset from which you want to remove physical resources and click **Edit**.
3. In the **Edit Dataset** window, click **Physical Resources** for the node from which you want to remove physical resources.
4. In the Edit Physical Resources page, select each resource you want to remove from the list and move it to the Available Resources list.

If you selected Physical Resources for the primary dataset node, the list is called Resources in this Dataset. If you selected a backup or mirror node, the list is called Resources in this Node.

5. Click **Next**.

The licensed application performs a trial run of your requested changes and generates a report describing the impact of those changes.

6. After you are satisfied with the preview results, click **Next** to apply your changes to the dataset, then click **Finish**.
7. Close the **Edit Dataset** window.

The licensed application removes the physical resources from the dataset.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Overview of export protocol properties

---

If you have the provisioning license installed, you can configure access for clients using NFS, CIFS, iSCSI, or Fibre Channel (FC) protocols when you create or reconfigure the primary, backup, or mirror nodes in your datasets or when you provision new volumes, LUNs, or qtrees as members into your datasets.

**CIFS access** To configure support for CIFS client access to the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The Windows domain of the target nodes in this dataset
- Specific permissions (full control, no access, or read and change) for specific users to access the nodes in this dataset

**NFS access** To configure support for NFS client access to the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node in the dataset and specify the following:

- Default permissions (Read only, read write, or root access) for all NFS hosts to access the selected node in this dataset
- Specific permissions for specific NFS hosts to access the selected node in this dataset
- The NFS security protocol (Kerberos v5 Integrity, Kerberos v5, Kerberos v5 Privacy, UNIX style, or None) that you want enforced
- A default mapping for anonymous users to the selected node
- Whether or not to enable superuser ID access to the selected node in this dataset

**Fibre Channel access** To configure support for FC client access to the SAN-based volumes, or LUNs in the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
- The World Wide Port Names for the FC nodes, if the accessing host does not have NetApp Host Agent installed

**iSCSI access** To configure support for FC client access to the SAN-based volumes or LUNs in the primary, backup, or mirror nodes in your dataset, you enable that access when you configure each node and specify the following:

- The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
- The initiator ID for the iSCSI nodes, if the accessing host does not have a NetApp Host Agent installed

#### Related concepts

[\*About NFS, CIFS, iSCSI, or FC protocol access\*](#) on page 699

[\*Decisions to make before provisioning a dataset\*](#) on page 729

[\*Dataset provisioning decisions\*](#) on page 714

#### Related tasks

[\*Displaying export properties for a specific dataset member\*](#) on page 417

# Configuring dataset nodes for CIFS protocol access

You can configure Windows client CIFS access to all NAS volumes or qtrees contained in a dataset's primary, backup, or mirror node if the dataset is configured to support CIFS access.

## Before you begin

- Confirm that the dataset node on which you want to enable CIFS access is assigned a NAS-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset you want to configure and click **Edit**.
3. In the **Edit Dataset** window, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify CIFS access.

If no provisioning policy has been assigned to this dataset, specify a NAS-type provisioning policy. The licensed application displays the provisioning policy assigned to the dataset node, and if that policy is a NAS-type policy, displays a CIFS Settings bar.
4. If the CIFS settings are not displayed, click the down arrow button on the CIFS Export Settings bar to expand the display.
5. Configure the CIFS settings. If CIFS is turned off, click **Turn CIFS On** to enable the settings.
6. Modify any other CIFS protocol or resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, and click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Configuring dataset nodes for NFS protocol access

You can configure NFS host access to all NAS volumes or qtrees contained in a dataset's primary, backup, or mirror node if the dataset is configured to support NFS access.

## Before you begin

- Confirm that the dataset node on which you want to enable NFS access is assigned a NAS-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual volumes or qtrees as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify NFS access.  
If no provisioning policy is assigned to this dataset, specify a NAS-type provisioning policy.  
The licensed application displays the provisioning policy assigned to the dataset node, and, if that policy is a NAS-type policy, displays an NFS Settings bar.
4. If the NFS settings are not displayed, click the down arrow button on the NFS Export Settings bar to expand the display.
5. Configure the NFS settings. If NFS is turned off, click **Turn NFS On** to enable the settings.
6. Modify any other NFS protocol or resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.  
If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Configuring dataset nodes for FC protocol access

You can configure Fibre Channel protocol (FC) client access to all SAN LUNs contained in a dataset's primary, backup, or mirror node if the dataset is configured to support FC access.

## Before you begin

- Confirm that the dataset node on which you want to enable FC access is assigned a SAN-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Note:

- FC is *not* supported on vFiler units
- If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify FC access.

If no provisioning policy has been assigned to this dataset, specify a SAN-type provisioning policy.

The licensed application displays the provisioning policy assigned to the dataset node. If that policy is a SAN-type policy, it displays an FCP Settings bar.

4. If the FC settings are not displayed, click the down arrow button on the FCP Export Settings bar to expand the display.
5. Configure the FC settings. If FC is turned off, click **Turn FCP On** to enable the settings.  
If iSCSI is turned on, it is automatically turned off when you click Turn FCP on.
6. Modify any other protocol and resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.

9. Close the **Edit Dataset** window.

**Related concepts**

*[About NFS, CIFS, iSCSI, or FC protocol access](#)* on page 699

**Related references**

*[Administrator roles and capabilities](#)* on page 1055

# Configuring dataset nodes for iSCSI protocol access

You can configure iSCSI client access to all SAN LUNs contained in a dataset's primary, backup, or mirror node if the dataset is configured to support iSCSI access.

## Before you begin

- Confirm that the dataset node on which you want to enable iSCSI access is assigned a SAN-type provisioning policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

**Note:** If you want to enable unique sets of export protocols on individual LUNs as you provision them into this dataset node, do not complete this task. Leave this dataset node with no export protocol enabled.

## Steps

1. Click **Data > Datasets > Overview**.
2. In the **Datasets** window, select the dataset that you want to configure and click **Edit**.
3. In the **Properties** sheet, click **Provisioning/Resource Pools** under the name of the node for which you want to enable or modify iSCSI access.

If no provisioning policy has been assigned to this dataset, specify a SAN-type provisioning policy. The licensed application displays the provisioning policy assigned to the dataset node. If that policy is a SAN-type policy, it displays an iSCSI Settings bar.
4. If the iSCSI settings are not displayed, click the down arrow button on the iSCSI Export Settings bar to expand the display.
5. Configure the iSCSI settings. If iSCSI is turned off, click **Turn iSCSI On** to enable the settings. If FCP is turned on, it is automatically turned off when you click **Turn iSCSI on**.
6. Modify any other resource pool settings. When you are finished, click **Next**.
7. Modify the vFiler unit configurations, as needed, then click **Next**.
8. If the Preview Details page shows no warnings or errors, click **Next**, then click **Finish**.

If the Preview Details page shows errors, follow the suggestions to fix the problems. You can click **Back** to change the settings on any page of the wizard.
9. Close the **Edit Dataset** window.

## Related concepts

[About NFS, CIFS, iSCSI, or FC protocol access](#) on page 699

**Related references**

*Administrator roles and capabilities* on page 1055

# Editing dataset general properties

You can edit the general properties of an existing dataset, as well as the dataset's physical resources, provisioning policy, export settings, and resource pools.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset that you want to modify then click **Edit**.
3. In the **Edit Dataset** window, use the menu to click the property that you want to modify.

If you want to modify...	Then...
The name, description, or volume and qtree name prefix of the dataset	Click <b>General Properties</b> .
The physical resources of the dataset's primary data	Under Primary data, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's primary data	Under Primary data, click <b>Provisioning/Resource Pools</b> .
The physical resources of the dataset's backup data	Under Backup, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's backup data	Under Backup, click <b>Provisioning/Resource Pools</b> .
The physical resources of the dataset's mirror data	Under Mirror, click <b>Physical Resources</b> .
The provisioning policy, export settings, or resource pools of the dataset's mirror data	Under Mirror, click <b>Provisioning/Resource Pools</b> .

4. Modify the dataset properties as needed, then click **Finish** to return to the **Edit Dataset** window.

The application saves your changes. If you modified the dataset name, the new name is displayed on the **Datasets** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a dataset

---

You can delete a dataset if you want to stop protection or disaster recovery for all of its members and stop conformance checking against its assigned protection and disaster recovery policies.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Overview**.
2. Select the dataset that you want to delete and click **Delete**.

The Delete Dataset dialog box opens, requesting that you confirm the deletion.

**Note:** When you delete a dataset, the physical resources that compose the dataset are not deleted.

3. Click **Yes** to confirm the delete request or **No** to cancel the request and close the dialog box.

The licensed application removes the dataset from the list in the **Datasets** window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# **Viewing volume, LUN or qtree space allocation**

---

You can use the **Datasets** window Provisioning tab to view current space usage for individual volume, LUN, or qtree members and historical space usage for individual volumes of a selected dataset.

## **Before you begin**

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. edit volume, LUN, or qtree configurations.

## **Steps**

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data > Datasets > Provisioning** to display it.
2. Select the dataset that contains the volume, LUN, or qtree whose space allocations you want to view.
3. Select the volume, LUN, or qtree whose space usage you want to view.

The licensed application displays the space allocation information for the selected volume, LUN, or qtree.

- Current space allocation is displayed on the Space breakout tab.
- Historical space allocation is displayed on the Space usage history tab.

**Note:** Historical space allocation is displayed for volumes and qtrees only.

## **Related concepts**

[Dataset storage space management](#) on page 705

## **Related references**

[Administrator roles and capabilities](#) on page 1055



# Diagnosing volume or qtree space status

---

You can use the Provisioning tab to view troubleshooting information and suggested actions for volumes or qtrees that display a Warning or Error space status.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data > Datasets > Provisioning** to display it.

The Provisioning tab displays a table of all datasets that you are authorized to administer.

2. Click the filter arrow on the Space Status column to list datasets with Warning or Error Space statuses.

The listed datasets are likely to require space allocation diagnosis and reconfiguration.

3. Select a listed dataset.

The Provisioning tab displays the volumes and qtrees contained in the selected dataset.

4. Select the volume or qtree displaying Warning or Error space status.

The Provisioning tab displays the space allocation information for the selected volume or qtree.

5. In the Volume section on the Current space breakout tab, click the  button to the right of the Space Status Warning, or Space Status Error icon.

The Provisioning tab displays the Space Status Details dialog box for the Warning or Error status in question.

6. View or copy the details.
  - To view more information click **Expand Errors and Warnings**.
  - To copy the troubleshooting information click **Copy to Clipboard**.

7. Click **OK** to exit the Space Status Details dialog box.

## Related concepts

[Dataset storage space management](#) on page 705

**Related references**

*Administrator roles and capabilities* on page 1055

# Resizing volume space

---

You can use the Provisioning tab to resize or reallocate data and Snapshot copy space in selected volumes.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data > Datasets > Provisioning** to display it.
2. Select the dataset that contains the volume whose space allocations you want to view.  
The Provisioning tab displays the volumes and qtrees contained in the selected dataset .
3. Select the volume that you want to resize and click the **Resize Storage** button.

**Note:** You cannot resize an imported storage element unless that element is imported from a resource pool that is already assigned to the containing dataset.

Depending on the type (NAS or SAN) of volume, the following parameters might be displayed for modification:

- Total volume size
  - Snap reserve %
  - Auto grow limit
4. Modify the Total volume size or Snap reserve % values by selecting new values or by dragging the related graph lines up or down in the space allocation simulation graph.
  5. After you specify your resizing, click **Resize** to finalize the new allocation.

## Related concepts

[Dataset storage space management](#) on page 705

[Space management resize options](#) on page 707

## Related references

[Administrator roles and capabilities](#) on page 1055



# Resizing qtree space

---

You can use the space management feature to resize individual qtree quotas.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data ▶ Datasets ▶ Provisioning** to display it.
2. Select the dataset that contains the qtree whose group quota you want to view.  
The Provisioning tab displays the volumes and qtrees contained in the selected dataset
3. Select the qtree that you want to resize and click the **Resize Storage** button.  
**Note:** You cannot resize an imported storage element unless that element is imported from a resource pool that is already assigned to the containing dataset.
4. Specify a new size, either in the Quota for Qtree parameter or by dragging the related graph line up or down in the space allocation simulation graph.
5. After you specify your resizing, click **Resize**.

## Related concepts

[Dataset storage space management](#) on page 705

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting Snapshot copies

---

You can use the space management feature to delete Snapshot copies from individual volumes in order to make more volume space available for data.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data > Datasets > Provisioning** to display it.
2. Select the dataset that contains the volume on which you want to delete Snapshot copies.

The Provisioning tab displays the volumes, LUNs and qtrees contained in the selected dataset.

3. Select the volume whose Snapshot copies you want to manage and click the **Delete Snapshot Copies** button.

The Delete Snapshot Copies dialog lists the Snapshot copies on the selected volume and the following information for each copy:

- Size. The amount of space this copy uses.
- Time created. When this copy was created.
- State. The origin or deletability of this copy.

The Snapshot copy can be in one of the following states:

- Normal. This Snapshot copy is the result of events not scheduled through the licensed protection application.
- Backup. This Snapshot copy is the result of backup or mirror activity configured through the licensed application.
- Cannot be deleted. This Snapshot cannot be deleted for space-saving purposes.
- Dependency. Whether this copy is in use by other active storage elements.

4. Select the Snapshot copies that you want to delete. To select more than one, hold down **Ctrl** while selecting your Snapshot copies with your cursor.
5. To view the amount of space that deleting your selected Snapshot copies frees in the selected volume, click **Calculate**.

The Delete Snapshot Copies dialog displays the amount of space to be freed.

**Note:** If the amount of space to be freed is insufficient, select additional Snapshot copies to delete and click **Calculate** again.

6. When the amount of space to be freed is sufficient, click **Delete** to execute deletion of the selected Snapshot copies.

#### Related concepts

[\*Dataset storage space management\*](#) on page 705

#### Related references

[\*Administrator roles and capabilities\*](#) on page 1055

# Deleting a volume, LUN or qtree

---

You can use the **Datasets** window Provisioning tab to delete volumes, LUNs, or qtrees, returning the space they use to their containing aggregates or volumes.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. If the Provisioning tab is not already displayed, from the navigation pane, click **Data** ▶ **Datasets** ▶ **Provisioning** to display it.
2. Select the dataset that contains the volume, LUN, or qtree that you want to delete.
3. Select the volume, LUN, or qtree that you want to delete.

The licensed application displays the space allocation information for the selected dataset member.

4. Click **Delete Storage** and click **OK** to confirm the deletion.

- If you delete a volume, the licensed application returns the space used by that volume to its containing aggregate.
- If you delete a LUN, the licensed application returns the space used by that LUN to its containing volume or containing qtree.
- If you delete a qtree, the licensed application returns the space used by that qtree to its containing volume.

## Related concepts

[Dataset storage space management](#) on page 705

## Related references

[Administrator roles and capabilities](#) on page 1055



# Dataset migration overview

---

You can migrate a dataset only if all the storage for the dataset is provisioned through a single vFiler unit. In addition, that vFiler unit must contain all the volumes for the dataset and no other volumes, with the exception of the root volume or root qtree. Therefore, you migrate a dataset when your storage strategy is focused on datasets; you migrate a vFiler unit when your storage strategy is focused on vFiler units.

When you create a dataset, you can specify an existing vFiler unit or you can have the provisioning application create a new vFiler unit for the dataset.

Migration of a dataset through a vFiler unit automatically migrates the following:

- NFS exports (however, you must remount the qtree-level exports for qtrees that are assigned to the vFiler unit when the vFiler unit contains a volume that belongs to the hosting storage system)
- CIFS shares (clients experience the equivalent of a reboot)
- igrroups
- LUN mappings
- Quota settings for the vFiler unit
- Backup and mirror relationships
- Backup versions
- DataFabric Manager history

Before you begin the migration cutover operation, you must shut down all applications that use the dataset.

## Related concepts

[Description of migration tasks](#) on page 955

[Dataset provisioning decisions](#) on page 714



# Dataset migration requirements

---

A dataset must meet the following requirements before you can migrate it to another storage system.

- The dataset has a vFiler unit attached to it through which all storage is provisioned.
  - Volumes and qtrees owned by another storage system cannot be members of the dataset.
  - Aggregates, other storage systems, Open Systems SnapVault hosts, and directories cannot be members of the dataset.
  - The vFiler unit is running Data ONTAP 7.3.1 or later.
- The attached vFiler unit has no other dataset attached to it.
- All storage systems owned by the vFiler unit, except for the root storage, belong to the dataset.
- The primary node of the dataset is not failed over.
- The dataset export protocol is either NFS or iSCSI.

## Related concepts

[\*Strategies for enabling a dataset for migration\*](#) on page 779

[\*Dataset provisioning decisions\*](#) on page 714



## Dataset migration and failover

---

The following rules apply to datasets that have policies assigned that are disaster recovery capable.

- A failed-over node of a dataset cannot be migrated.
- Failover operations are allowed on a dataset at any time, regardless of whether data migration is in progress.
- If a data migration is in progress when a dataset node fails over, the data migration operation is automatically canceled.



# Dataset migration limitations

---

The following limitations apply to data migration.

- Primary storage

For datasets, only the dataset primary node can be migrated.

- Secondary storage

vFiler units owning secondary storage (any volume that is the destination of a SnapVault or SnapMirror relationship) cannot be migrated.

- SnapMirror schedules

The data migration update process does not manage the SnapMirror schedules of the relationships. Instead, it relies on the default schedules created by the Migrate Start operation, which causes the subsequent SnapMirror updates to be controlled by the target storage system. The default for scheduled migration updates is every three minutes. The migration cutover operation optionally modifies the SnapMirror relationships to synchronous mode.

If you want to use a different schedule, use the Operations Manager DR tab to modify the schedule.

- Throttles

Throttles are not migrated and are not supported.

- SnapMirror connections

SnapMirror connections are not supported.

- Effect of Protection Manager

If the Protection Manager license is not installed, the dataset migration is limited as follows:

- The migration relationships are not periodically monitored. Therefore, the relationship lag is not updated.

- The SnapMirror and SnapVault relationships are not migrated.

- VLANs and IPspaces

- The provisioning application does not configure partner interfaces for preexisting interfaces.

- VLANs and IPspaces of the source vFiler unit are not deleted automatically during the migration cleanup operation. You must manually delete any VLANs and IPspaces.

- Failure of the migration cutover operation

If the migration cutover operation fails, the source vFiler unit is left in a stopped state. When the provisioning application automatically starts the source vFiler unit, some clients may be disrupted.

- vFiler units with qtree root storage

The migration process can successfully migrate a vFiler unit that has the root storage in a qtree that is contained in a volume that is not owned by that vFiler unit. However, the backup versions of that root storage qtree are not migrated.

- vFiler units with IPv6 addresses

vFiler units with IPv6 address cannot be migrated.

- qtree-level NFS exports

After a migration is finished, you must remount any qtree-level NFS exports that were configured on the source vFiler unit for qtrees that were assigned to the vFiler unit and were contained by a volume that belonged to the hosting storage system.

- vFiler unit quotas

Quotas enforced on the source vFiler unit from the hosting storage system are not migrated.

- vFiler unit routes

The migration process does not migrate routes configured on the vFiler unit; you must manually configure the routes on the destination storage system. If all of the following conditions apply, the migration is transparent and you must manually configure the routes on the destination storage system:

- The migration cutover or migration cleanup process is finished.

- The migrated vFiler unit is in nondefault IPspace.

- That IPspace does not exist on the destination storage system.

- Maximum number of vFiler units on a storage system

Each storage system has a maximum number of vFiler units allowed; this limits the number of migration-capable datasets that can be provisioned from the storage system. On high-end storage system models, the hard limit is approximately 64.

- Role-based access control (RBAC)

Roles created for the source vFiler unit are not migrated. You must manually create the roles on the target vFiler unit.

## Related concepts

[\*Description of migration tasks\*](#) on page 955

[\*When to relinquish the migration capability of a dataset\*](#) on page 777

# When to relinquish the migration capability of a dataset

---

When provisioning a dataset or starting a dataset migration, you might encounter a message that the maximum number of vFiler units has been reached. When this occurs, you might need to relinquish the migration capability of one or more datasets.

Each storage system imposes a limit on the number of vFiler units it can support, and that limit can be very low (maximum of 64 on high-end storage systems). Because the licensed provisioning application creates additional vFiler units when a migration-capable dataset is provisioned or migrated, you might quickly reach the maximum allowed when provisioning or migrating a dataset with that capability. To resolve the problem, you might need to relinquish the migration capability of some older or less important datasets.

You can only relinquish the migration capability of datasets for which a vFiler unit was created when the dataset was first added. When you select a dataset in the **Datasets** window Migration tab, the "Relinquish migration capability" button is enabled for datasets that meet this requirement.

**Note:** When you relinquish the migration capability of a dataset, the provisioning application destroys the vFiler unit assigned to the dataset and reexports all of the data to the storage systems associated with the dataset.

## Related concepts

[Dataset migration limitations](#) on page 775

## Related tasks

[Relinquishing migration capability of a dataset](#) on page 797



# Strategies for enabling a dataset for migration

---

Any dataset that meets the dataset migration requirements is enabled for automated offline migration; no additional configuration is required. However, there are two strategies for enabling a dataset for automated offline migration.

## Strategy 1: When adding a new dataset, allow the wizard to create a vFiler unit

1. When you add a new dataset, you can enter an IP address and a network mask on the Transparent Migration page of the **Add Dataset** wizard. The licensed provisioning application creates a new vFiler and assigns it to the dataset.
2. Export all provisioned storage for the dataset through that single vFiler unit.

## Strategy 2: Assign an existing vFiler unit to a dataset

1. Create a vFiler unit and add it as a host.
2. Assign the vFiler unit to the dataset.
  - If you are adding a new dataset, you can assign an existing vFiler unit on the vFiler unit page of the **Add Dataset** wizard.
  - If the dataset already exists, you can assign an existing vFiler unit by editing the Provisioning and Resource Pools configuration of the dataset.
3. Export all provisioned storage for the dataset through that single vFiler unit.

## Related references

[Dataset migration requirements](#) on page 771

[Administrator roles and capabilities](#) on page 1055



# **Decisions to make before starting dataset migration**

---

Before starting a dataset migration operation by using the **Dataset Migration** wizard, it is useful to have ready all the migration information for the dataset and associated vFiler unit.

**Dataset migration** Are you migrating a dataset or a vFiler unit?

**commands or  
vFiler unit  
migration  
commands**

- If there is a direct one-to-one correspondence between a dataset and a vFiler unit, you may use either the dataset migration commands or the vFiler unit migration commands.
- If a vFiler unit contains more than one dataset, you should use the vFiler unit migration commands.
- If a vFiler unit contains more than one dataset, but the storage for at least one of the datasets is owned by more than one vFiler unit, you should use the dataset migration commands for each separate dataset.

**Destination  
storage system**

What is the destination storage system for the migrated dataset?

You can select a resource pool or a storage system as a destination.

- If the vFiler unit attached to the dataset was created automatically when the dataset was added, then you can select a resource pool and the provisioning application selects the best storage system.
- If the vFiler unit attached to the dataset was not created automatically when the dataset was added (it was assigned after the dataset was created), then you must select a storage system and provide the network binding information.

**Destination  
provisioning  
policy**

Which provisioning policy do you want applied to the migrated dataset?

By default, the currently assigned provisioning policy for the source dataset is selected; however you can select a different one.

**Interface  
selections**

If the vFiler unit for the dataset was assigned after the dataset was created, then you need to provide interface information.

- What vFiler unit interface and VLAN ID do you want to use?  
If the vFiler unit associated with the dataset was not created using the default Interface settings and if the destination storage system has a default Interface configured, then which interfaces do you want configured? You can select from a list of already-populated IP addresses that displays the associated Netmask and Interface values, and the already-populated VLAN ID of each. You can also modify the VLAN ID.

**Note:** If you provisioned the vFiler unit automatically when you added the dataset (using the **Add Dataset** wizard) but now you want to associate the vFiler unit to a VLAN and configure the interface IP failover, you must first use the **Setup vFiler Unit** wizard to edit the configuration of the vFiler unit before starting the **Dataset Migration** wizard.

- What vFiler unit interface and VLAN ID do you want to use in the partner storage system?  
If the destination storage system is configured as active/active, you also need to specify an IP address in case IP failover occurs.

#### Related concepts

[\*Description of migration tasks\*](#) on page 955

#### Related tasks

[\*Starting a dataset migration\*](#) on page 783

# Starting a dataset migration

---

You can begin data migration for a dataset by initiating the migrate start operation, which starts the **Dataset Migration** wizard and begins a baseline data transfer.

## Before you begin

Have the information available that you need to complete this task:

- Destination storage system (required)
- Provisioning policy for destination storage system (optional)
- Interface to which the IP address will be bound to the destination storage system and the VLAN ID (required only for a dataset with a vFiler unit that was assigned after the dataset was created)
- Physical VLAN interface on which the VLAN will be created if VLANs are created during migration for the partner of the destination storage system (required if the destination storage system has an active/active configuration)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can cancel a dataset migration anytime during the migration start operation.

## Steps

1. From the navigation pane, click **Data > Datasets > Migration**.
2. Select a dataset and click **Start migration** to start the **Dataset Migration** wizard.
3. Complete the pages of the wizard then confirm the details of the migration and click **Finish** to complete the wizard.

You can check the job progress displayed in the Tracking Dataset Migration Job display popup window or in the Jobs tab on the **Datasets** window Migration tab.

At any time after the migration start operation finishes successfully, you can update the SnapMirror relationships by initiating the migration update operation.

## After you finish

To continue the migration, you must manually initiate the migration cutover operation.

## Related concepts

[Decisions to make before starting dataset migration](#) on page 781

*Description of migration tasks* on page 955

**Related tasks**

*Updating dataset migration SnapMirror relationships* on page 785

*Cutting over to the new dataset storage destination* on page 787

*Canceling a dataset migration* on page 791

**Related references**

*Administrator roles and capabilities* on page 1055

# Updating dataset migration SnapMirror relationships

After the migration start operation finishes, you can initiate an on-demand update of the SnapMirror relationships that were created as part of the migration start operation. This is an optional step in the dataset migration process,

## **Before you begin**

You can perform this task only on a dataset that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## **About this task**

This operation is useful if a scheduled update fails, which causes the lag time of the SnapMirror relationships to increase to an undesirable length.

## **Steps**

1. From the navigation pane, click **Data > Datasets > Migration**.
2. Select a dataset and click **Update** to update the SnapMirror relationships that were created as part of the migration start operation.
3. Click **Yes** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Datasets** window Migration tab Jobs tab, or in the **Jobs** window.

## **After you finish**

To continue the migration, you must manually initiate the migration cutover operation at a convenient time.

## **Related concepts**

[\*Description of migration tasks\*](#) on page 955

## **Related tasks**

[\*Starting a dataset migration\*](#) on page 783

[\*Cutting over to the new dataset storage destination\*](#) on page 787

**Related references**

*Administrator roles and capabilities* on page 1055

# Cutting over to the new dataset storage destination

After the migration start operation finishes, you can initiate the migration cutover operation to switch the old destination from which the data is served to the new destination and update the SnapMirror relationships.

## Before you begin

- You can perform this task only on a dataset that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.
- Because this is an automated offline migration, you must shut down all applications that use the dataset.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You might want to initiate this operation at a time when the dataset has a very low level of activity. When the migration cutover operation begins, you cannot cancel or reverse it.

## Steps

1. From the navigation pane, click **Data > Datasets > Migration**.
2. Select a dataset and click **Cutover**.
3. (Optional) In the confirmation dialog box, you can enter the name of a script to be executed.

For example, a script might quiesce an application and then resume the application after the cutover is performed.

4. Click **Cutover** in the confirmation dialog box to begin the operation.

After the dataset is switched over to the destination storage system, the backup versions, backup relationships, and DataFabric Manager history for the volumes are transferred to the destination storage system.

## After you finish

- To continue the migration, you must manually initiate the migration cleanup operation.
- You must restart all applications that use the migrated dataset.

## Related concepts

[Description of migration tasks](#) on page 955

**Related tasks**

*Starting a dataset migration* on page 783

*Updating dataset migration SnapMirror relationships* on page 785

*Cleaning up a dataset migration* on page 789

**Related references**

*Administrator roles and capabilities* on page 1055

# Cleaning up a dataset migration

---

After the migration cutover operation finishes, you can initiate the migration cleanup operation to delete the volumes that were used by the vFiler unit on the old data storage system.

## Before you begin

You can perform this task only on a vFiler unit that has the status "Migrated, cleanup required." This status indicates that the migration cutover operation is finished.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Migration**.
2. Select a dataset and click **Cleanup**.

The Migration Cleanup confirmation dialog box lists the volumes on the old destination that will be deleted.

3. Click **Apply** to begin the operation.

## After you finish

To complete the migration process, you must manually perform the following cleanup tasks using an application like FilerView (if the VLANs and IPspaces are not shared):

- Dynamic references in the old source dataset
- VLANs and IPspaces used by the old source vFiler unit

## Related concepts

[\*Description of migration tasks\*](#) on page 955

## Related tasks

[\*Cutting over to the new dataset storage destination\*](#) on page 787

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Canceling a dataset migration

---

You can cancel a dataset migration at any time when the status is "started, cutover required." When you cancel a dataset migration, the licensed provisioning application aborts all ongoing transfers and deletes all the provisioned storage on the destination storage system and on the destination vFiler unit.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Datasets > Migration**.
2. Click **Cancel**.
3. In the confirmation dialog box, click **Yes**.

## After you finish

After you cancel a dataset migration, you must manually delete the VLANs and IPspaces that were created on the destination storage system and vFiler unit.

## Related tasks

[\*Starting a dataset migration\*](#) on page 783

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Viewing dataset migration status

---

You can view the status of a dataset migration operation in the **Datasets** window Migration tab.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Step

1. From the navigation pane, click **Data > Datasets > Migration**.

The status is displayed in the "Migration status" column.

## Related references

*[Administrator roles and capabilities](#)* on page 1055



# **Environment variables for data migration scripts**

---

Use the following environment variables when you write premigration and postmigration scripts for dataset and vFiler unit migration.

- PM\_CUTOVER\_MODE

This variable indicates whether the script is to be executed before or after the switch to the new destination. Valid values are as follows: PM\_BEFORE\_CUTOVER and PM\_AFTER\_CUTOVER.

- Information about the source dataset or vFiler unit:

- PM\_SOURCE\_VFILER\_ID
- PM\_SOURCE\_VFILER\_NAME
- PM\_SOURCE\_FILER\_ID
- PM\_SOURCE\_FILER\_NAME

- Information about the destination dataset or vFiler unit:

- PM\_DEST\_VFILER\_ID
- PM\_DEST\_VFILER\_NAME
- PM\_DEST\_FILER\_ID
- PM\_DEST\_FILER\_NAME

- Information about the dataset:

- PM\_DATASET\_ID
- PM\_DATASET\_NAME



# Relinquishing migration capability of a dataset

---

You can relinquish the migration capability of a dataset by removing the vFiler unit assignment for the dataset.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

When provisioning a dataset, or starting a dataset migration, you might encounter a message that the maximum number of vFiler units has been reached. When this occurs, you might need to relinquish the migration capability of one or more datasets.

**Note:** This operation destroys the attached vFiler unit and relinquishes the contained resources (for example, the volumes, the qtrees, the quotas, and the NFS, CIFS, and iSCSI exports to the hosting storage system).

## Steps

- From the navigation pane, click **Data > Datasets > Migration**.

You can also relinquish the migration capability of a dataset in the **Edit Dataset** window.

- Select a dataset that has a vFiler unit assigned and for which you want to remove the migration capability, and click **Relinquish migration capability**.

The "Relinquish migration capability" button is enabled only for datasets that have an attached vFiler unit that was created when the dataset was first added.

The provisioning application performs a test of the modification and lists all resulting errors and warnings in the **Preview Details** window.

- In the confirmation dialog box, click **Relinquish**.

## Related concepts

[When to relinquish the migration capability of a dataset](#) on page 777

## Related tasks

[Adding a dataset](#) on page 719

## Related references

[Administrator roles and capabilities](#) on page 1055



# What deduplication is

---

Deduplication is a provisioning application option that you can enable on your storage nodes to eliminate duplicate data blocks to reduce the amount of storage space used to store active data.

On the affected volumes, deduplication allows you to reduce the amount of space used to store active data, or even allows you to purposely over deduplicate and store more bytes of data than the capacity of the available physical storage.

You can enable your provisioning policies to support three modes of deduplication.

<b>On-demand deduplication</b>	On-demand deduplication is executed on a selected volume that is enabled for deduplication when you click the <b>Dedupe Now</b> button on your Provisioning tab.
<b>Automated</b>	Automated deduplication, if enabled on a dataset node, is run automatically on any volume in that node when the amount of new data written to that volume reaches 20%.
<b>Scheduled deduplication</b>	Scheduled deduplication, if enabled on a dataset node, is run automatically on the volumes in that node on the days of the week, during a particular time period, and at a frequency that you have specified.

## Related concepts

[How the protection application supports deduplication](#) on page 593



# Deduplication configuration requirements

---

You can enable deduplication for both SAN and NAS containers that reside on storage systems that meet configuration requirements.

To support the Management console's deduplication feature, the managed storage systems must meet the following configuration requirements:

- Data ONTAP 7.2.4 or later is installed.

**Note:** Data ONTAP 7.3 or later is required to support deduplication on volumes on a vFiler unit.

- The Deduplication license is installed.
- The NearStore personality license is installed.

**Note:** This license is not required for R200 storage systems or storage systems running Data ONTAP 7.3.1 or later.

- Storage system-specific and Data ONTAP version-specific maximum volume sizes for deduplication are observed.

**Note:**

- Scheduled deduplication is not supported on SnapVault or volume SnapMirror destinations.
- If deduplication is enabled on a volume on which Autogrow and Snapshot autodelete are enabled and fractional reserve is disabled, writes cannot be guaranteed on that volume.
- To ensure against partial failure of SnapVault-based or Qtree SnapMirror-based backup operations from an over deduplicated primary volume to a secondary volume of the same size, you can enable the protection application's global `dpDynamicSecondaryResize` option in Operations Manager.

Enabling the protection application for dynamic resizing of backup volumes allows a backup volume to dynamically resize its physical capacity in the event that the logical amount of over deduplicated data being transferred from its primary volume exceeds the secondary volume's original physical size.

For more information about deduplication-supported maximum volume sizes on various storage systems running various versions of Data ONTAP, see the latest version of the NetApp Deduplication for FAS and V-Series Deployment and Implementation Guide (TR-3505) .

## Related information

*NetApp Deduplication for FAS and V-Series Deployment and Implementation Guide - <http://media.netapp.com/documents/tr-3505.pdf>*



# What happens during deduplication

---

After deduplication is enabled and started, the provisioning application performs a full or incremental consolidation of duplicate data blocks on the volumes on which deduplication has been applied.

- The deduplication process is triggered by one of three possible events:
  - If the "On-demand deduplication" mode is enabled on a dataset node, deduplication is run on-demand by the user on a selected volume.
  - If the "Automated deduplication" mode is enabled on a dataset node, deduplication begins automatically on a volume residing on that dataset node when the amount of new or changed data on that volume reaches 20%.
  - If the "Scheduled deduplication" mode is enabled on a dataset node, deduplication begins automatically according to a user-customized schedule on all volumes in a dataset node.

**Note:** In "Scheduled deduplication" mode, deduplication starts on Disaster Recovery capable Mirror destinations only after the SnapMirror relationship between primary storage and the secondary storage nodes on which they reside is broken.

- The initial deduplication operation on a volume is a full volume run. All blocks of data on the volume are scanned for duplication and the duplicate blocks are consolidated (or deduplicated).

**Note:** Because the initial deduplication operation is a full volume run, in which all data is scanned, it requires more time to complete than subsequent operations.

- Subsequent deduplication operations are usually incremental operations. Only the new or changed blocks of data on the target volume or volumes are scanned for duplication and possible consolidation.

**Note:** In "On-demand deduplication" mode, you have the option of starting a full volume or partial volume run every time you click **Dedupe Now**.



# Over deduplication

---

Over deduplication is the effective deduplication-enabled storage of more logical bytes of data in a volume or aggregate container than are actually allotted to that container. The measure of over deduplication can be expressed as a percentage of volume capacity or as a percentage of aggregate capacity.

**Over  
deduplication  
in a volume**

Over deduplication in a volume is expressed as a percentage of the deduplication-enabled logical stored data in a volume over the actual physical capacity of that volume.

This percentage is calculated as:  $100 \times (\text{logical stored data} \div \text{total volume size})$

**Note:** Logical stored data = used volume space + deduplication saved space

As an example of over deduplication on a volume, consider a deduplication-enabled volume of 100GB with no Snapshot reserve. If the user fills that volume with 80GB of data (consisting of eight common files of 10GB each) and runs deduplication on that volume, the user sees a deduplication space saving of 70GB and a used volume space of 10GB.

If the user fills the volume with an additional 70GB of data (again consisting seven 10GB files consisting of the same common data as above), and deduplication is re-run, the second deduplication run gives the user an additional deduplication space savings of 70GB, and the used space in volume is still 10GB.

In this case: used volume space = 10GB; deduplication saved space = 140GB

So the logical stored data = 150GB on a total volume size of 100GB.

Over deduplication for the volume =  $100 \times (150\text{GB} \div 100)$  which is 150%

**Over  
deduplication  
in an  
aggregate**

Over deduplication in an aggregate is expressed as a percentage of total logical stored data over the total aggregate size.

This percentage is calculated as:  $100 \times (\text{total logical stored data} \div \text{total aggregate size})$

**Note:**

- Total logical stored data is the sum of the logical stored data of each deduplication-enabled volume in the aggregate.
- The logical stored data on a volume is calculated differently for volumes with different space guarantees.
- On volumes with volume space guarantee, the logical stored data is calculated as the total volume size or as used space plus deduplication saved space, whichever is greater.

- On volumes with file guarantee enabled, logical stored data is calculated as the sum of used space and deduplication saved space.
- On volumes with no space guarantee enabled, the logical stored data is calculated as the sum of the used space and the deduplication saved space.

As an example of over deduplication for an aggregate, consider a 1TB aggregate consisting of 5 volumes, 3 of those volumes deduplication-enabled, with deduplication-enabled space savings as follows:

- Volume A (volume guarantee): 200GB Total size, 50GB Used space, 100GB Saved Space
- Volume B (file guarantee): 200GB Total size, 150GB Used space, 500GB Saved Space
- Volume C (none guarantee): 200GB Total size, 150GB Used space, 400GB Saved Space

So the total logical stored data is 200GB + 650GB + 550GB or 1400GB located on an aggregate of one TB or 1024GB.

The over deduplication for the aggregate is  $100 \times (1400\text{GB} \div 1024\text{GB})$  or 136%

**Note:** For calculating over deduplication percentage the Snapshot reserve is not counted since the data in the Snapshot reserve cannot be deduplicated.

## Over deduplication and backup protection

To ensure against partial failure of SnapVault-based or Qtree SnapMirror-based backup operations from an over deduplicated primary volume to a secondary volume of the same physical size, you can enable the protection application's global `dpDynamicSecondaryResize` option in Operations Manager

Enabling the protection application for dynamic resizing of backup volumes allows a backup volume to dynamically resize its physical capacity in the event that the logical amount of over deduplicated data being transferred from its primary volume exceeds the secondary volume's original physical size.

# Deduplication space savings percentage

---

Deduplication enables you to store more logical data using less physical storage space. The deduplication space savings percentage is the deduplication space savings over the logical used space on the volume or aggregate container minus that used space that is claimed for Snapshot reserve or overwrite reserve functions and cannot be deduplicated.

**Deduplication** Deduplication space savings is the absolute amount of space that is saved in a volume **space savings** or aggregate because of deduplication.

As an example of deduplication space savings on a volume, consider a deduplication-enabled volume of 100GB with no Snapshot reserve. If the user fills that volume with 80GB of data, which happens to consist of eight 10GB files consisting of the same common data, and runs deduplication on that volume, the user sees an actual used volume space of only 10GB and a deduplication space saving of 70GB.

If the user fills the volume with an additional 70GB of data (again consisting seven 10GB files consisting of the same common data as above), and deduplication is re-run, the second deduplication run gives the user an additional deduplication space savings of 70GB, and the used space in volume is still 10GB. So in total the deduplication space savings for that volume is 140GB.

**Volume  
Space  
Savings  
percentage**

The deduplication space savings percentage for a volume is expressed as a percentage of the deduplication space savings against the logical used volume data space.

The formula for calculating the deduplication space savings percentage for a volume is:

$$100 \times (\text{deduplication space savings} \div \text{logical used volume data space})$$

The logical used volume data space is calculated as follows:

- In NAS volumes, logical used volume data space = deduplication space savings + total volume space used – Snapshot reserve space – Snapshot overflow

**Note:** Snapshot reserve space and Snapshot overflow space cannot be deduplicated and so do not enter into the percentage calculation.

- In SAN volumes, logical used volume data space = deduplication space savings + total volume space used – Snapshot overflow - available overwrite reserve - the reserve hole..

**Note:** The Snapshot reserve space for SAN volumes is generally 0. Therefore, all the Snapshot data gets counted as Snapshot overflow. In addition to Snapshot overflow, the available overwrite reserve and the hole reserve are deducted from the total volume space used because these reserves cannot be deduplicated.

As an example, if NAS volume A, experiences a deduplication space saving of 50GB, an actual volume space usage of 75GB, a Snapshot reserve space of 10GB, a Snapshot overflow of 5GB, then the deduplication space savings percentage is  $100 \times 50\text{GB} \div (50\text{GB} + 75\text{GB} - 10\text{GB} - 5\text{GB})$  which calculates as 45%.

#### **Aggregate Space Savings percentage**

Aggregate space savings percentage is the percentage of total deduplication space savings in the aggregate against the logical used space of the aggregate.

The aggregate space savings percentage is calculated as follows:

$100 \times \text{aggregate deduplication space savings} \div \text{aggregate logical space used}$ .

- aggregate deduplication space savings = the total deduplication space savings in all the volumes contained in an aggregate.
- aggregate logical space used = the aggregate deduplication space savings + the total used space in all the volumes that have been enabled for deduplication in an aggregate.

For example, if Aggregate B, experiences an aggregate deduplication space saving of 500GB, an actual aggregate space usage of 750GB, a Snapshot reserve space usage of 50GB, a Snapshot overflow of 25GB, then the aggregate deduplication space savings percentage is  $100 \times 500\text{GB} \div (500\text{GB} + 750\text{GB} - 50\text{GB} - 25\text{GB})$  which calculates as 42%.

# Enabling deduplication on your dataset nodes

---

You can enable deduplication on a new or existing provisioning policy and then assign that policy to one or more dataset nodes. All volumes on that node are then enabled for deduplication.

## Before you begin

- Confirm that the provisioning application is licensed on the NetApp Management Console .
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

### 1. Enable deduplication on a new or existing provisioning policy.

- If you are enabling deduplication while creating a new provisioning policy, start and complete the **Add Provisioning Policy** wizard.

While completing the wizard, enable deduplication and specify the mode of deduplication (On-demand deduplication, Automated deduplication, or Scheduled deduplication) that you want to enable.

- If you are enabling deduplication on an existing provisioning policy, select, edit, and save that policy.

While editing the policy, enable deduplication and specify the mode of deduplication (On-demand deduplication, Automated deduplication, or Scheduled deduplication) that you want to enable.

### 2. Assign the provisioning policy on which you have enabled deduplication to the dataset node that contains the volumes or will contain the volumes on which you want to execute deduplication.

Depending on the mode of deduplication that you enabled, initial deduplication starts differently on the target volumes.

- If you enabled On-demand deduplication, deduplication starts when you navigate to the Provisioning tab, select the dataset and the volume on which you want to run deduplication, and click **Dedupe Now**.
- If you enabled Automated deduplication, deduplication starts on a volume when the amount of new data written to that volume since the last deduplication reaches 20% of volume capacity.
- If you enabled Scheduled deduplication, deduplication starts on the volumes in a dataset node on the days of the week, during a particular time period, and at a frequency that you have specified.

## After you finish

After deduplication is started, you can view the Deduplication tab to monitor the space saved on the volumes due to deduplication.

**Related tasks**

- [Editing a provisioning policy](#)* on page 879
- [Adding a provisioning policy](#)* on page 875
- [Assigning or changing a provisioning policy](#)* on page 727
- [Starting on-demand deduplication](#)* on page 813

**Related references**

- [Administrator roles and capabilities](#)* on page 1055

# Disabling deduplication on dataset nodes

---

You can disable deduplication for a set of volumes by editing the provisioning policy assigned to the storage node on which they reside.

## Before you begin

- Confirm that the provisioning policy that is assigned to the dataset node on which you want to disable deduplication is not also assigned to other dataset nodes on which you do not want to disable deduplication.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Step

1. To disable deduplication for a storage node, select, edit and save the provisioning policy assigned to that node. While editing the policy, deselect the deduplication option.

After deduplication is disabled on a dataset node, all deduplication on the volumes that reside on that node stops. Data blocks already deduplicated remain deduplicated, but no further deduplication is carried out.

**Note:** Later changes to currently deduplicated data blocks causes those blocks to unconsolidate and lose deduplication.

## Related tasks

[Editing a provisioning policy](#) on page 879

## Related references

[Administrator roles and capabilities](#) on page 1055



# Starting on-demand deduplication

---

You can start on-demand deduplication on any volume that resides on a dataset node that has been enabled for deduplication.

## Before you begin

- Ensure that the volume on which you want to start on-demand deduplication resides on a dataset node on which deduplication is enabled.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the Navigation pane click **Data ▶ Datasets ▶ Provisioning**.
2. Select the dataset that contains the volume on which you want to start deduplication.
3. Select the volume and click **Dedupe Now**.
4. When prompted specify whether to execute full-volume deduplication or partial volume deduplication.
  - Full volume deduplication scans all the data in the volume for possible deduplication.
  - Partial volume deduplication scans the new data since the last deduplication scan for possible deduplication.

Either full-volume or partial volume deduplication starts on the selected volume.

## Related tasks

[Enabling deduplication on your dataset nodes](#) on page 809

## Related references

[Administrator roles and capabilities](#) on page 1055



# Stopping an in-progress deduplication

---

You can stop deduplication that is in progress on a selected volume.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the Navigation pane click **Data > Datasets > Provisioning**.
2. Select the dataset that contains the volume on which you want to stop an in-progress deduplication.
3. Select the volume.  
If deduplication is in progress, the Abort deduplication button is active.
4. Click **Abort dedupe**.

Further deduplication on the selected volume stops. Data blocks already deduplicated by the stopped job remain deduplicated.

### Note:

- Later changes to the deduplicated data blocks unconsolidates those blocks, and the space-savings related to that deduplication is lost.
- Unless deduplication on the dataset node has been disabled, later on-demand, automated, or scheduled deduplication will restart or resume the deduplication on the selected volume.

## Related references

[Administrator roles and capabilities](#) on page 1055



# **Viewing volume-level deduplication space-saving**

---

You can view graphs that indicate the space saving that deduplication enables on selected volumes.

## **Before you begin**

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## **Steps**

1. From the Navigation pane click **Data ▶ Datasets ▶ Provisioning**.
2. Select the dataset that contains the volume on which you want to view deduplication-related space savings.
3. Select the volume and click the Deduplication tab.

The provisioning application displays a chart and explanation comparing storage space currently used by the selected volume with the storage space it would be using without deduplication enabled.

## **Related references**

*Administrator roles and capabilities* on page 1055



# Overview of resource pools

---

A resource pool is a collection of unused physical storage resources, such as aggregates and disks, grouped together based on a user-defined set of common attributes.

You might pool your resources based on attributes such as performance, cost, physical location, or availability. By grouping related resources into a pool, you can treat the pool as a single unit for monitoring, provisioning, reporting, and role based access control (RBAC). This simplifies the management of these resources and allows for a more flexible and efficient use of the storage.

You create resource pools by using the **Add Resource Pool** wizard, which is accessible from the **Resource Pools** window. By using the wizard, you can select from a list of available aggregates, entire storage systems, or groups of physical resources from which to create your resource pool.

After you create a resource pool, you can associate it with one or more datasets. You can also associate datasets with provisioning and protection policies. These tasks can be accomplished when you add or edit datasets from the **Datasets** window.

When you assign a data protection policy, the licensed protection application applies the policy settings to automatically provision destination volumes from the assigned resource pool. It then creates backup and mirror relationships from each volume and qtree in the dataset to the newly provisioned secondary storage.

When you assign a provisioning policy to a dataset node, the licensed provisioning application applies the availability characteristics and space settings in the policy to automatically select the resources needed to fulfill a request for storage space for the primary data of a dataset.

These relationships between physical storage units, resource pools, and datasets mean that you must consider carefully what the impact might be of changes made to the system.

## Related concepts

[Dataset concepts](#) on page 693

[Decisions to make before adding datasets](#) on page 711

[Ways you might combine resources in resource pools](#) on page 825

[What groups are](#) on page 1047

[Decisions to make before assigning or changing policies](#) on page 721

**Related references**

*Advantages of using resource pools* on page 821

# Advantages of using resource pools

---

By using resource pools, you can simplify physical storage resource management in several ways.

Some advantages of using resource pools are listed here:

- You can group various resources with similar attributes, providing a quick view of similar storage objects.
- Resource pools provide a single logical unit for provisioning.
- You can simplify physical resource management by managing a pool of resources as a single entity.
- You can configure your system to automatically provision storage from resource pools, without your intervention.
- You can create resource pools in advance of allocating them to datasets, so that the resource pools are available when needed.
- You can enable event generation on resource pools so that when a set threshold is crossed, an event is generated to alert the resource pool owner.
- You can assign a label to resource pools or members of resource pools.

This allows you to filter the resources available for provisioning to only those that have a specific label assigned to them.

**Note:** This feature is available only when the provisioning application is licensed.

## Related concepts

[\*Overview of resource pools\*](#) on page 819

[\*Ways you might combine resources in resource pools\*](#) on page 825



# Resource pool properties

---

You can use the following definitions when you configure or edit a resource pool's properties.

- [General Properties](#) on page 823
- [Physical Resources](#) on page 823
- [Labels](#) on page 824
- [Space Thresholds](#) on page 824

## General Properties

These properties are associated with the entire resource pool.

<b>Name</b>	The name assigned to a resource pool. Special characters and spaces are permitted in names. The limit is 64 characters, but for readability, it is best to keep the description under 25 characters
<b>Description</b>	A description of the resource pool. This description might include the intended use of the resource pool, the type of storage contained in the resource pool, or some other common attribute that identifies why the storage was grouped into a resource pool.  The limit is 255 characters, but for readability, it is best to keep the description under 40 characters.
<b>Owner</b>	The name of the person responsible for this resource pool. You can list multiple owners, delimited by commas. There is no formatting restriction.
<b>Contact (optional)</b>	The e-mail address of the person to contact if there are issues with the resource pool. You can have multiple e-mail contacts delimited by commas.
<b>Time Zone</b>	The time zone you want to assign to the resource pool.

## Physical Resources

These properties let you designate which available physical resources to include in this resource pool.

<b>Available physical resources</b>	A list of the physical resources available for assignment to this resource pool.
<b>Resources in this resource pool</b>	A list of physical resources already assigned to this resource pool.

## Labels

These optional properties let you assign optional labels to the resource pool or objects within the resource pool.

<b>Resource Label (optional)</b>	A user-assigned label associated with a resource pool or the objects in a resource pool. It essentially functions as a filter, allowing you to identify specific resources to be considered when fulfilling a provisioning request. A resource label is a text string of any length.
<b>Resources (optional)</b>	The names of the physical storage resources, such as hosts and aggregates, that are allocated to a resource pool.

## Space Thresholds

These optional properties let you designate space usage thresholds at which to generate events and send alarms related to this resource pool.

<b>Space Thresholds (optional)</b>	<p>Resource pool-related data storage measurements at which an event is generated.</p> <ul style="list-style-type: none"><li>• Resource Pool Nearly Full threshold and Resource Pool Full threshold These are thresholds used to track the amount of space consumed in a resource pool. Alerts are generated when these thresholds are reached. The default thresholds are: Nearly Full = 80%, Full = 90%</li><li>• Aggregate Nearly Overcommitted threshold and Aggregate Overcommitted threshold These are thresholds used to track the sum of committed space of all aggregates belonging to the resource pool. Alerts are generated when these thresholds are reached. Tracking these thresholds in an environment where the aggregates are overcommitted (thin provisioning) is particularly important, because in such an environment administrators commit more storage than is physically available. The default thresholds are: Nearly Overcommitted = 300%, Overcommitted = 400%</li></ul>
--	--

## Related tasks

[Adding a resource pool](#) on page 841

[Editing resource pool properties](#) on page 845

## Related references

[Resource pool guidelines](#) on page 831

# Ways you might combine resources in resource pools

---

Prior to creating resource pools, consider how you will be using the available storage. This will help you to determine how you want to combine those resources into resource pools to meet your setup's replication needs.

Following are examples of ways that you might combine your physical resources to make the most efficient use of your resource pools:

- A set of aggregates composed of inexpensive, slow, ATA drives  
This pool is suitable for archival or compliance purposes, but it is not appropriate for mission-critical, high-performance database applications.
- A set of high-performance aggregates composed of 15K Fibre Channel disk drives in a RAID-DP configuration  
This pool is suitable for enterprise-critical applications.
- A set of resources categorized based on cost or performance  
This pool might be given a simple designation, such as *Gold*, *Silver*, or *Bronze*.
- A set of storage systems that are suitable for provisioning for certain departments within an organization
- A set of homogenous resources grouped together as a way of restricting access to high-performance storage

## Related concepts

[Overview of resource pools](#) on page 819

## Related references

[Advantages of using resource pools](#) on page 821



## Sequence for selecting backup destination volumes

If an existing backup relationship already has a volume assigned to contain backup data, the licensed protection application tries to use it. Otherwise, the application selects an existing volume that meets certain requirements or, if necessary, provisions a new destination volume.

For data residing on storage systems, the size estimate for destination volumes that are provisioned by the protection application is 1.2 times the size of the volume containing the protected data. The destination aggregate must have at least this much available space.

**Note:** Whenever possible, the protection application uses FlexVol volumes when provisioning backup destination volumes. The application implements aggregate overcommitment, observing the Aggregate Overcommitted and Aggregate Nearly Overcommitted thresholds specified in Operations Manager. For more information about aggregate overcommitment, see the *Operations Manager Administration Guide* and the *Data ONTAP Storage Management Guide*. For information about the aggregate overcommitment thresholds, see the Operations Manager online Help.

For data residing on Open Systems SnapVault clients, the licensed protection application uses a projected size of 100 GB for the destination volume.

To be considered as a destination for backups, a volume must be on a storage system configured with the appropriate Data ONTAP licensing to store backups.

From the pool of volumes that meet these requirements, the protection application takes the following steps to select a destination volume for backups:

1. The application looks for secondary volumes associated with the dataset that already have a relationship originating from the primary volume.  
However, if a secondary volume has too many relationships, the application excludes that volume from the selection process. The default maximum number of relationships is 50.
2. Of the secondary volumes associated with the dataset that have a pre-existing relationship with the primary volume, the application looks for a destination that has enough space to satisfy the projected space requirement of the primary data.
3. If none of the secondary volumes with pre-existing relationships with the primary volume can satisfy the space requirement, the application scans the destination systems for an existing FlexVol volume with adequate space and no SnapVault or Qtree SnapMirror relationships.
4. If the protection application cannot locate an existing FlexVol volume with adequate space and no SnapVault or Qtree SnapMirror relationships, it scans the destination systems for existing traditional volumes with adequate space and no SnapVault or Qtree SnapMirror relationships.
5. For systems running Data ONTAP 7.0 or later, if the protection application cannot find a volume with adequate space and no existing SnapVault relationships, it attempts to provision a FlexVol volume.
6. If the application cannot provision a FlexVol volume, it generates an error.

**Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## **Sequence for selecting mirror destination volumes**

To find a suitable destination to contain mirrored data, the licensed protection application tries to use the same volume used for the existing mirror relationship, if there is one. Otherwise, the application selects an existing volume that meets certain requirements or, if necessary, provisions a new destination volume.

If the protection application needs to provision a new volume to contain mirrored data, the new volume is provisioned to be the same size as the aggregate in which it resides.

**Note:** If the application provisions a mirror destination volume on a tertiary node, the new volume is provisioned to be the same size as the secondary volume even if the secondary volume is larger than the tertiary aggregate. Space guarantees for the new volume are disabled.

The licensed protection application takes the following steps to select a destination volume for mirror copies:

1. If there is no existing mirror relationship, the application scans the destination systems for an existing volume that meets the following requirements:
  - Is located on a storage system running the same or later Data ONTAP version as the storage system containing the data to be mirrored
  - Is located on a storage system on which the SnapMirror license is enabled
  - Is of the same type (FlexVol or traditional volume) as the volume containing the data to be mirrored
  - Is the same size or larger than the source volume
  - Has no SnapVault or SnapMirror relationships
2. If the application cannot locate an existing volume that meets the preceding requirements, it attempts to use available space in the resource pool to provision a new volume of the same type as the volume containing the data to be mirrored. For the protection application to provision a new volume, the aggregate or spare disk where the new volume is created must meet the following requirements:
  - Belongs to a storage system running the same or later Data ONTAP version as the storage system containing the data to be mirrored
  - Belongs to a storage system on which the SnapMirror license is enabled
  - Has adequate space for the data in the source volume
3. If the application cannot provision a new volume for the data to be mirrored, it generates an error.



# Resource pool guidelines

---

These guidelines can help you optimize the advantages of using resource pools.

## Content and structure of resource pools

- Resource pools cannot nest and cannot overlap (that is, storage in one resource pool cannot be in another resource pool).
- Resource pools can be members of DataFabric Manager groups, but resource pools cannot contain DataFabric Manager groups.
- Resource pools can be created from entire storage systems or from aggregates.
- Adding a storage system to a resource pool implies that all existing aggregates and spare disks on the storage system are included as part of that pool, along with any new aggregates that are created.
- Members of a resource pool do not all need to reside on the same storage system or .
- A storage system can be designated as a resource pool that contains a mixture of resources with various attributes.
- A storage system or an aggregate can only belong to one resource pool at a time.
- Individual aggregates within the same storage system can belong to different resource pools as long as the storage system as a whole has not been assigned to a resource pool.

## Considerations when selecting storage for resource pools

- When creating a resource pool, you determine which storage elements to include in the pool based on one or more common properties, such as "all storage in the same building" or "all storage delivering the same level of performance."
- Adding an aggregate to a resource pool allows the application to create new volumes by using the aggregate's free space.  
When provisioning resources, the aggregate's preexisting volumes are not used.
- When provisioning resources for primary data, you can choose to increase the available space in an existing volume by deleting Snapshot copies or by assigning additional space for the volume. LUNs cannot be resized.  
In a NAS environment, space can be grown and Snapshot copies deleted only manually. In a SAN environment, these tasks can be done manually, but they can also be done automatically by using a provisioning policy.
- Access to a resource pool is controlled via role-based access control (RBAC), so in some deployments you might want to group homogeneous resources together as a way of restricting access to high performance storage. In other deployments you might construct resource pools with a mix of storage attributes as a means of providing better storage utilization across an organization.

- Systems running on Data ONTAP versions earlier than 7.0 cannot use the aggregate or flexible volume features. This impacts how you assign destination resources for mirrored copies and backups.

**Mirrors** If you are mirroring data, you can only select entire storage systems to include in resource pools. The licensed protection application uses the spare disks on the storage systems to provision traditional volumes for the mirrored copies.

**Backups** The licensed protection application cannot provision resources for backup jobs. You must, manually create the volumes to add to the dataset's secondary node. When you assign resources to a dataset, only the volumes are available for selection.

#### **Provisioning from resource pools**

- When a resource pool contains a storage system, all aggregates on the storage system are available for provisioning.
- Both traditional and flexible volumes can be created from a resource pool. However, flexible volumes are available only when running systems on Data ONTAP 7.0 or later.
- Aggregates are used for provisioning of flexible volumes for Data ONTAP 7.0 or after. Spare disks are used for provisioning of traditional volumes by the administrator, for Data ONTAP versions prior to 7.0.
- When using the licensed protection application, you cannot control how specific volumes are provisioned from resource pools. The application evaluates available resources for a number of criteria, such as valid login credentials, working NDMP, ONTAP version, licenses, and so forth. From the aggregates that pass those filters, the application picks the aggregate with the most free bytes as the one to hold the backup.

#### **Naming and labeling resource pools**

- You are advised to name resource pools according to the characteristics of the storage each resource pool contains.
- The name is limited to 64 characters. However, for readability, it is advised that names be no longer than 25 characters. You can use any combination of letters, numbers, or special characters in resource pool names.
- Use a label name that has significant meaning. A label should only be used when you want to more narrowly control the resources being provisioned. For example, if you want to restrict the provisioned resources by their cost and performance, you might assign a label of Tier-1, Tier-2, or Tier-3. If a Tier-1 resource label is selected for a provisioning policy and a provisioning action occurs, only those resources assigned to the dataset and labeled as Tier-1 will be considered for provisioning.

**Note:** The Label property is only available when the provisioning license is installed.

**Status of resource pools** The status of a resource pool is equivalent to the worst status of any event pools associated with any member of that resource pool.

#### Related concepts

*[Decisions to make before adding a resource pool](#)* on page 837

#### Related tasks

*[Adding a resource pool](#)* on page 841

*[Editing resource pool properties](#)* on page 845

#### Related references

*[Resource pool properties](#)* on page 823



## How resource labels work

---

You can assign a resource label as a way to narrow the available resources to be considered for a provisioning request. This feature is only available when the provisioning application is licensed.

The resource label can be assigned when you create a resource pool. This is an optional custom property that you can assign to a resource pool or to the individual storage systems or aggregates that comprise the resource pool. You might assign a resource label based on factors such as cost, reliability, or specific configurations. The resource label essentially functions as a filter. It allows you to identify specific resources to be used to fulfill a provisioning request, so that only those resources that have the label assigned to them are considered. This allows finer control when matching provisioning requests with available resources.

When you create a provisioning policy, you can specify a resource label to be associated with the policy. If a label is specified for a policy, only the resource pools and resource pool members that match the label are used when a provisioning request is fulfilled using that policy. However, storage that has an assigned resource label can still be used to fulfill provisioning requests that do not specify a label.

For example, assume an administrator assigns a resource label of **Tier-1** to a resource pool containing the highest-cost, most reliable storage. The administrator also creates a provisioning policy named prov-pol-1, with the resource label **Tier-1** specified. When a provisioning request is made on a dataset that has the prov-pol-1 policy assigned to it, the provisioning application searches for storage that uses the **Tier-1** label. If no resources with that resource label are available, the provisioning request fails. For this reason, you should use resource labels with care.



## Decisions to make before adding a resource pool

---

Before creating a resource pool by using the **Add Resource Pool** wizard, it is useful to have all the resource pool configuration information ready.

- |                                   |  |
|-----------------------------------|--|
| <b>Name<br/>(required)</b>        | What name do you want to assign to the resource pool? <ul style="list-style-type: none"><li>• Provide a meaningful name that briefly describes the storage or the intended use of the storage in the resource pool.<br/>An example of a name that describes the storage path is: <code>server1_homedirs</code>, <code>tier1_mktg</code>, or <code>china_eng</code>.</li><li>• Special characters and spaces are permitted in names.<br/>The limit is 64 characters, but for readability, it is advised that you keep the name under 25 characters.</li></ul> |
| <b>Description<br/>(optional)</b> | How do you want to describe the resource pool, so the intended use of the resource pool is clear? <ul style="list-style-type: none"><li>• Provide a meaningful description of the resource pool, such as an explanation of the intended use of the resource pool.</li><li>• The limit is 255 characters, but for readability, it is advised that you keep the description under 40 characters.</li></ul>   |
| <b>Owner<br/>(optional)</b>       | Who should be contacted regarding problems with the resource pool? <ul style="list-style-type: none"><li>• Provide the name of the person or people responsible for maintaining this resource pool.</li><li>• You can list multiple owners, delimited with a comma. There is no formatting restriction.</li></ul>  |
| <b>Contact<br/>(optional)</b>     | Who should be alerted regarding problems with the resource pool? <ul style="list-style-type: none"><li>• Provide the e-mail addresses or e-mail aliases to which notifications, alerts, and so forth should be sent concerning the resource pool.</li><li>• The e-mail addresses listed here might be the same ones used for receiving alerts regarding the resource pool.</li><li>• You can have multiple e-mail contacts, delimited with a comma.</li></ul>  |
| <b>Time Zone<br/>(required)</b>   | Will you use the default time zone for the resource pool or change the time zone? <ul style="list-style-type: none"><li>• The resource pool must have a time zone selected. You can retain the default setting or change it.</li></ul>   |

To select a time zone, you can either scroll through the entire list or type a time zone designation in the Filter Time Zone text box.

<b>Physical Resources (required)</b>	<p>How will you determine which storage to include in the resource pool from the list of physical resources available?</p> <ul style="list-style-type: none"><li>Decide on which properties you want to base the creation of the resource pool: for example, location, cost, performance, reliability, or access privileges.</li><li>Decide whether the resource pool will contain individual aggregates, an entire storage system (all the aggregates in a storage system), or a combination.</li><li>Decide which version of Data ONTAP will run on the systems in this resource pool.<ul style="list-style-type: none"><li>Note that systems running Data ONTAP versions earlier than 7.0 cannot use the aggregate or flexible volume features. This impacts how you later assign destination resources for mirror copies and backups.</li></ul></li><li>Decide if you want to use traditional volumes or flexible volumes in the resource pool.<ul style="list-style-type: none"><li>Flexible volumes are available only when running Data ONTAP 7.0 or later.</li><li>Aggregates are used for provisioning of flexible volumes, and spare disks are used for provisioning of traditional volumes.</li><li>If you intend to associate a resource pool with a data set in a mirror relationship, the volumes on the primary node and those on the secondary nodes must be of the same type. You cannot combine traditional volumes and FlexVol volumes on nodes that are part of a mirror relationship.</li></ul></li><li>Decide how much available storage space you need for the resource pool, based on the resource pool's intended use.</li><li>Verify that you have the appropriate software licenses on the storage you intend to use.</li></ul>
<b>Labels (optional)</b>	<p>When a provisioning request is processed, do you want to restrict the resources available for provisioning to only those with a specific label assigned to them?</p> <ul style="list-style-type: none"><li>A label set on an individual member of a resource pool takes priority over a label applied to the entire resource pool.</li><li>The labels can be edited inline in the table. For both resource pool and members, an existing label can be selected from the drop-down list or a new label can be typed in.</li></ul>

<b>Space Thresholds (optional to modify default)</b>	<p>At what point do you want to receive alerts regarding consumption of space in the resource pool?</p> <ul style="list-style-type: none"><li>• Resource Pool Nearly Full threshold and Resource Pool Full Threshold This set of thresholds can be used to track the amount of space consumed in a resource pool. Alerts are generated when these thresholds are reached.</li><li>• Aggregate Nearly Overcommitted threshold and Aggregate Overcommitted threshold This set of thresholds can be used to track the sum of committed space of all aggregates belonging to the resource pool. Alerts are generated when these thresholds are reached. Tracking these thresholds in an environment where the aggregates are overcommitted (thin provisioning) is particularly important, because in such an environment administrators commit more storage than is physically available.</li></ul>
--	---

#### Related concepts

[\*Effect of time zones on schedules\*](#) on page 1049

[\*Protection policy node prerequisites\*](#) on page 1051

#### Related tasks

[\*Adding a resource pool\*](#) on page 841

#### Related references

[\*Resource pool guidelines\*](#) on page 831



# Adding a resource pool

---

You can create resource pools from collections of unused physical storage resources. Resource pools are associated with one or more datasets, providing the physical resources for provisioning primary storage by using a provisioning policy and also for backup or mirror protection on nonprimary nodes.

## Before you begin

Ensure that the hosts you are adding to the resource pool have the proper configuration and licensing for their intended use.

Have the information available that you need to complete this task:

- Name that you want assigned to the resource pool (required)
- Description of the resource pool (optional)
- Owner of the resource pool (optional)
- Contact e-mail address for anyone receiving alerts about the resource pool (optional)
- Time Zone used for actions involving the resource pool (optional to select a time zone other than the default)
- Physical Resources to associate with the resource pool (required)
- Resource Pool Label used for filtering resources during provisioning (optional)
- Space Thresholds for setting alerts for out-of-space conditions (optional to modify the default)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Resource Pools**.
2. Click **Add** to open the **Add Resource Pool** wizard and then complete the wizard.
3. Verify the creation and content of the resource pool by viewing the results that are displayed in the **Resource Pools** window.

## After you finish

You can use the **Datasets** window to associate the new resource pool with a new or existing dataset.

- If you want to associate a resource pool with a new dataset, use the **Add Dataset** wizard.
- If you want to associate a resource pool with an existing dataset, use the **Edit Dataset** window.

If you want to modify any of the properties of a resource pool, click **Edit** in the **Resource Pools** window.

## **Related concepts**

[\*Decisions to make before adding a resource pool\*](#) on page 837

[\*Effect of time zones on schedules\*](#) on page 1049

## **Related tasks**

[\*How do I back up data?\*](#) on page 589

## **Related references**

[\*Resource pool properties\*](#) on page 823

[\*Data ONTAP licenses used for protecting or provisioning data\*](#) on page 905

[\*Administrator roles and capabilities\*](#) on page 1055

[\*Resource pool guidelines\*](#) on page 831

# **Impact of modifying resource pool properties**

---

Before making changes to the properties of a resource pool, you need to understand the potential impact of those changes on your data protection setup.

Editing the Name, Description, Owner, or Contact properties for a resource pool does not impact the functioning of a resource pool; it only modifies the information viewed about the resource pool. However, editing the members or the time zone of a resource pool can have a significant impact on your data. The impact of modifying the membership of an existing resource pool depends on whether the resource pool is already associated with a dataset.

## **Modifying a resource pool that is *not* associated with a dataset**

Editing any of the properties of a resource pool that is not associated with a dataset does not impact any protected data. However, if you are modifying the resources or time zone of a resource pool, consider the potential result before making the change.

- Will the new size and number of aggregates be adequate for the intended use of the resource pool?
- Will a time zone change affect the schedule synchronization between the primary storage data and the secondary storage backup or mirror copy?

## **Modifying a resource pool that *is* associated with a dataset**

- |   |   |
|---|---|
| <b>Modifying the members of a resource pool</b> | <ul style="list-style-type: none"><li>• Adding or removing the resources of a resource pool might affect the size and number of aggregates available for provisioning, once the resource pool is associated with a dataset.</li><li>• Removing resources: If an entire storage system is assigned to a resource pool, as aggregates are added to or removed from that storage system, the aggregates are automatically added to or removed from the resource pool that the storage system is associated with. You do not need to perform any additional tasks to have the aggregates available for provisioning.</li><li>• Adding resources: Verify that any resource you plan to add to a resource pool is online, properly configured, and licensed for the purpose you intend for it.<br/>Adding a resource that is not available for provisioning can result in lack of conformance. For example, if an aggregate you plan to add is nearly full, the application cannot provision from that aggregate and jobs involving that aggregate will fail.</li></ul> |
|---|---|

- |   |   |
|---|---|
| <b>Modifying the time zone of a resource pool</b> | <ul style="list-style-type: none"><li>• Does not affect data that is already protected.</li></ul> |
|---|---|

- Might affect whether the replication schedule on the primary dataset synchronizes as expected with the schedule on secondary or tertiary destination storage in the resource pool.

## Related concepts

[\*Effect of time zones on schedules\*](#) on page 1049

## Related tasks

[\*Editing resource pool properties\*](#) on page 845

# Editing resource pool properties

---

You can edit the properties of an existing resource pool by using the Edit properties option, accessible from the **Resource Pools** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance. edit resource pool settings, such as the `GlobalFullControl` role.

Have the information available that you need to complete this task, depending on which properties you intend to edit:

- Settings
  - Name you want assigned to the resource pool
  - Description of the resource pool
  - Owner of the resource pool
  - Contact e-mail addresses for the people or aliases to alert regarding problems
  - Time Zone used for the resource pool
- Resources  
Be sure the resources you add to the resource pool have the proper configuration and licensing for their intended use.
- Labels to be associated with the resource pool or the aggregates
- Space Thresholds
  - Nearly full threshold
  - Full threshold
  - Nearly overcommitted threshold
  - Overcommitted threshold

## Steps

1. From the navigation pane, click **Data > Resource Pools**.
2. In the list of available resource pools, select the resource pool that you want to modify.
3. Click **Edit** to open the **Properties** sheet.
4. Modify the properties that you want changed.
5. Click **OK**.
6. Verify the changes to the resource pool properties.

You can verify the changes by viewing the information displayed in the **Resource Pools** window.

The resource pool's properties configuration is modified and saved.

### **After you finish**

Verify that any data set associated with the modified resource pool is still in conformance with any assigned provisioning or protection policies.

### **Related concepts**

*[Impact of modifying resource pool properties](#)* on page 843

### **Related references**

*[Resource pool properties](#)* on page 823

*[Administrator roles and capabilities](#)* on page 1055

# What a policy is

---

A policy is a set of rules that specifies the intended management of dataset members. You can apply the same policy to multiple datasets, leveraging your configuration of the policy across the datasets. If you update a policy, the update is propagated across all the datasets to which the policy is applied. Different types of policies address different data management issues.

Depending on the licenses you have installed, the data management applications provide the following types of policies:

- Protection without disaster recovery
- Protection with disaster recovery
- Provisioning
- vFiler templates

**Note:** The data management policies used by applications running in NetApp Management Console should not be confused with other kinds of policies, such as the file policies used in Data ONTAP.

## Next topics

- [\*What a protection policy is\* on page 847](#)
- [\*What a provisioning policy is\* on page 848](#)

## Related concepts

- [\*Dataset concepts\* on page 693](#)

# What a protection policy is

Protection policies define how protection relationships should be structured and the property settings for each component of the structure. If you also have the Disaster Recovery license, protection policies can also define how to fail over to secondary storage on the disaster recovery node when disaster occurs.

When a protection policy is applied to a dataset, it defines how data stored in dataset members should be backed up or mirrored. You can configure a protection policy that specifies a single protection method (local backup, remote backup, or mirroring) or a combination of those methods. For example, a protection policy might specify that the primary data is backed up to a secondary location and that the secondary copies are mirrored to a tertiary location.

If the Disaster Recovery license is installed, protection policies that use Qtree SnapMirror to back up data can also invoke your site's disaster recovery script. After the problem is resolved, you can move dataset member access manually from the secondary storage back to the primary storage.

## **Related concepts**

- [\*Decisions to make before adding datasets\* on page 711](#)
- [\*Dataset protection decisions\* on page 711](#)
- [\*Decisions to make before assigning or changing policies\* on page 721](#)
- [\*Types of data protection\* on page 235](#)
- [\*Protection policy nodes and connections\* on page 237](#)
- [\*Retention of hourly, daily, weekly, and monthly backups\* on page 241](#)
- [\*Protection policy node prerequisites\* on page 1051](#)
- [\*Allowable lag times\* on page 247](#)
- [\*Protection schedules and time zones\* on page 301](#)

## **Related tasks**

- [\*Assigning or changing a protection policy\* on page 725](#)

## **Related references**

- [\*Protection policies \(not disaster recovery capable\)\* on page 669](#)

# **What a provisioning policy is**

Provisioning policies define the desired features of NAS or SAN storage for datasets, including reliability/availability, space management settings, and appropriate actions when a storage container needs more space. The policy settings specify how you want to have storage provisioned, exported and managed for the datasets to which you apply the policy.

A provisioning policy applies to all volumes, qtrees, or LUNs in a dataset node; you cannot assign different policies to individual members within a dataset. This is different from protection policies which can be assigned to individual volumes, qtrees, or LUNs in a dataset node.

A dataset can have a single node or, if you also have the Protection license and you assign a multi-node protection policy to it, a dataset can have a primary and secondary (or even tertiary) node. If you also have the Protection license and the dataset has a mirror or backup node, you can create and assign policies that define the provisioning of storage on the secondary and tertiary node.

## **Related concepts**

- [\*Difference between provisioning policy and provisioning wizard\* on page 851](#)
- [\*Decisions to make before adding datasets\* on page 711](#)
- [\*Dataset provisioning decisions\* on page 714](#)
- [\*Dataset protection decisions\* on page 711](#)





## Difference between provisioning policy and provisioning wizard

---

A provisioning policy governs the out-of-space actions, export protocols, and so on for a dataset. The **Provisioning** wizard adds new volumes, qtrees, or LUNs to an existing dataset.

When a storage container runs out of space, the actions taken are determined by the provisioning policy: the licensed application might send space warning messages and, for SAN storage, might try to increase the container size or delete old Snapshot copies, or both. The policy does not direct the application to create new volumes, qtrees, or LUNs.

When you create a dataset for provisioning and assign a provisioning policy, the licensed provisioning application creates a single storage container in the associated resource pool, according to the policy settings.

You can create and add new volumes or LUNs to a dataset by using the **Provisioning** wizard.

### Example scenario

- A storage administrator needs to create a dataset for the home directories of all the users in the accounting department. The home directories are CIFS shares; each user is allowed 50 GB.
  - The administrator creates a dataset named AccountingUserDirectories and assigns a provisioning policy that has the correct CIFS export settings.
  - The licensed application creates one container for the dataset from the associated resource pool, according to the properties in the provisioning policy.
- When a new employee joins the accounting department, the administrator needs to add another volume on the existing dataset and assign a CIFS share for that employee.
  - The administrator uses the **Provisioning** wizard to add a new volume in the resource pool associated with the dataset.
- As the data in the user directories fills up the assigned storage, the administrator needs to provision more storage space.
  - When the data reaches a Nearly Full or Full threshold, the provisioning policy automatically sends an event message, if that action is configured.
  - The administrator can manually change the volume size or can use the **Provisioning** wizard to add additional volumes to the dataset.

**Related concepts**

*What a provisioning policy is* on page 848

# Provisioning policy properties

---

These descriptions of provisioning policy properties include where property values can be edited or viewed, and any special considerations regarding the property.

- [Where to view and modify property values](#) on page 853
- [General properties](#) on page 853
- [Availability properties](#) on page 854
- [NAS container properties](#) on page 854
- [SAN container properties](#) on page 855
- [Provisioning script](#) on page 856
- [Resource label](#) on page 856
- [Deduplication Properties](#) on page 856
- [Deduplication Properties](#) on page 856
- [Space utilization thresholds](#) on page 856

## Where to view and modify property values

You can specify, view, and modify property values as follows:

- You can initially set a value for a property in the **Add Provisioning Policy** wizard.
- You can view a policy property in the **Provisioning Policies** window. To display a hidden column, you click  in the upper-right corner of the jobs list and select the column.
- You can modify a policy property in the **Properties** sheet, which is accessed by clicking **Edit** in the **Provisioning Policies** window.

## General properties

<b>Name</b>	The name assigned to a provisioning policy. Name is a required property.  Special characters and spaces are permitted in names. The limit is 64 characters, but for readability, it is recommended that you keep the name under 25 characters.
<b>Description</b>	A description of the provisioning policy. It might include the intended use of the provisioning policy or some other common attribute that identifies why the provisioning policy was created. Description is an optional property.

**Storage Type** The type of storage the policy is configured to support. Storage type is a required property and cannot be modified:

<b>NAS</b>	The licensed application provisions NAS storage on a primary node and exports storage for NAS access. NFS and CIFS protocols are supported.
<b>SAN</b>	The licensed application provisions SAN storage on a primary node and exports storage for SAN access. FCP and iSCSI protocols are supported.
<b>Secondary</b>	The licensed application provisions storage on a secondary node for use as destinations for backup and mirror operations. This type is available only if you have the Protection license also installed.

## Availability properties

The storage availability properties are related to various aggregate and storage controller configurations. These properties are optional; if none is configured then a provisioning request provisions from any available storage resource in the resource pool. The availability levels that datasets might require are as follows:

<b>RAID-DP (Double disk failure)</b>	The application looks for storage resources configured using RAID-DP aggregates to protect data from double disk failures. This is the default value.
<b>RAID4 (Single disk failure)</b>	The application looks for storage resources configured using RAID4 aggregates to protect data from single disk failures. This option is the default if no reliability level is specified.
<b>Storage subsystem failure (aggregate SyncMirror)</b>	The application looks for storage resources using SyncMirror aggregates to protect data from failures of adapters, cables, and shelves.
<b>Storage controller failure (active/active configuration )</b>	The application looks for storage resources using an active/active configuration to protect data from controller failures.

## NAS container properties

<b>Quota settings</b>	The default size of user quotas and group quotas. Quotas limit resource usage and provide notification when resource usage reaches specified levels. Quota sizes can be specified in units of KB, MB, GB, or TB. Quotas are an optional property.
-----------------------	---

<b>Space utilization properties</b>	The actions the licensed application takes to manage space for dataset members and Snapshot copies. Space utilization is an optional property.
<b>Guarantee space for data and Snapshot copies</b>	If this option is enabled, the space is guaranteed for data and for Snapshot copies and guaranteed from the resource pool(s) associated with the dataset. Writes to a specified FlexVol volume or writes to files with space reservations enabled do not fail due to a lack of available space in the containing aggregate.  If this option is disabled, the space is allocated on-demand as data or Snapshot copies are written to datasets; some write requests might fail.
<b>Reserve space for Snapshot copies</b>	If this option is enabled, an additional 20 percent of the requested space is provisioned from the resource pool(s) for Snapshot copies for every provisioned member in the dataset. This guarantees that Snapshot copies do not fail because of a lack of disk space.  If this option is disabled, no additional Snapshot copy space is provisioned and Snapshot copies might fail if there is not enough space available.

## SAN container properties

<b>Type of containers to provision as dataset members</b>	The SAN container type to be used for provisioning: Volume or LUN. Container type is a required property.	
<b>Space for data</b>	<b>Guaranteed</b>	Space for data is guaranteed on the SAN container.
	<b>On demand</b>	Space for data is not guaranteed on the SAN container. Space might need to be allocated manually.
<b>Space for Snapshot copies</b>	<b>Guaranteed</b>	Space for Snapshot copies is guaranteed on the SAN container.
	<b>On demand</b>	Space for data is not guaranteed on the SAN container; the container is automatically increased when additional space for Snapshot copies is needed.
<b>Delete oldest Snapshot copies automatically</b>	If this option is enabled and a SAN container needs more space, the Data ONTAP autosize option is used to automatically delete Snapshot copies to make more space available. To use these option, your storage must be using Data ONTAP 7.2.4 or later.	

If this option is disabled, Snapshot copies are not automatically deleted when a SAN container needs more space, therefore, you might need to delete them manually.

## Provisioning script

The full path on the DataFabric Manager server of a provisioning script that performs custom tasks after storage is provisioned. Provisioning script is an optional property.

## Resource label

A text string that is used to match provisioning requests with available resources. Only storage resources that match the label are used for provisioning. Because resource labels limit the available resources for provisioning requests, you should use them sparingly. Resource label is an optional property.

## Deduplication Properties

Whether you want to enable block-level deduplication on the volumes that reside of the dataset node to which this policy is assigned and if so which deduplication mode that you want to apply.

**On-demand deduplication** Deduplication runs only when you select a volume on the dataset node on which this mode is selected and click **Dedupe Now**.

**Automated deduplication** Deduplication runs automatically on any volume that resides on the current dataset node after that volume contains 20 percent new data written to it since the last deduplication run.

**Scheduled deduplication** Deduplication runs automatically on a custom schedule that you have specified for all volumes that reside on the current dataset node. You can schedule deduplication to run on which days of the week, during what time period, and at what frequency.

## Space utilization thresholds

Whether the application generates space utilization events when a threshold is reached. The application uses these thresholds to compute dataset space status and generate events. Space thresholds are optional properties.

**Generate space utilization events** If this option is enabled, event notifications are generated when a space threshold is reached.  
If this option is disabled, no event notifications are generated when a space threshold is reached.

**Full threshold** The percentage of the maximum size of a dataset at which a Full threshold event notification is generated. You can enter the percentage number or slide the indicator up or down to the appropriate percentage. The default is 90 percent.

**Nearly Full threshold** The percentage of the maximum size of a dataset at which a Nearly Full threshold event notification is generated. You can enter the percentage number or slide the indicator up or down to the appropriate percentage. The default is 80 percent.

#### Related concepts

[\*Decisions to make before adding a provisioning policy\*](#) on page 861

#### Related tasks

[\*Adding a provisioning policy\*](#) on page 875

[\*Editing a provisioning policy\*](#) on page 879



# Viewing a provisioning policy

---

You can view all the provisioning policies and their properties in the **Provisioning Policies** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > Provisioning**.
2. Click the Details tab at the bottom of the screen.

## Related references

*Administrator roles and capabilities* on page 1055



# Decisions to make before adding a provisioning policy

---

Before you start the **Add Provisioning Policy** wizard, you need to gather the information required to complete the wizard.

**How many volumes are currently in the dataset?** The licensed provisioning application can manage a maximum of 50 volumes in a dataset. If a dataset currently has a storage resource that contains more than 50 volumes, the provisioning request fails.

**General policy information**

- What is the name and description of the policy?
- What is the type of storage you want to provision with this policy? Will the policy be used to provision and export storage for NAS access (NFS or CIFS protocols) on a primary node, or for SAN access (FCP or iSCSI protocols) on a primary node? If you also have a protection license, you can use the policy to provision storage for a secondary node (backup or mirror destination).

**Storage availability (optional)** Does the dataset require a specific level of storage availability? If so, the application tries to find resources that provide the specified availability. (Only the specified availability is selected; storage with a higher level of availability will not be selected.) The default is to protect or provision data from any available storage resource. The choices are:

- RAID-DP (Double disk failure)  
The application provisions from storage resources that are configured using aggregate RAID-DP.
- RAID4 (Single disk failure)  
The application provisions from storage resources that are configured using aggregate RAID4.
- Externally managed RAID  
The application provisions from V-Series storage. Therefore, RAID protection is determined by the V-Series storage capabilities.
- Storage subsystem failure (aggregate SyncMirror)  
The application provisions from storage resources that use aggregate SyncMirror.
- Storage controller failure (active/active configuration )  
The application provisions from storage resources that have an active/active configuration.

<b>Resource label (optional)</b>	<p>Do you need to filter for specific resources for provisioning?</p> <p>If so, what text string do you want to use for the resource filter? The licensed provisioning application uses that text string (the resource label) to match provisioning requests with available resources that are configured with the same resource label. (Resource labels should be used sparingly because they limit the available resources for provisioning requests.)</p>
<b>Deduplication</b>	<p>Do you want data deduplication enabled on the volumes residing in the dataset node to which this provisioning policy is applied? If so, what kind of deduplication do you want to enable?</p> <ul style="list-style-type: none"><li>• Do you want only to run deduplication manually? If you decide to configure this option, deduplication starts only when you manually select a volume and click the <b>Dedupe Now</b> button.</li><li>• Do you want enable auto deduplication? If you decide to enable auto deduplication, deduplication automatically starts on a volume that resides on this dataset node when that volume contains 20% new data written to it since the last deduplication run.</li><li>• Do you want to attach a custom schedule for deduplication? If you decide to schedule deduplication, you can specify deduplication to start on which days of the week, during what time period, at what frequency, and during that time period.</li></ul>
<b>NAS container properties</b>	<ul style="list-style-type: none"><li>• Quotas What is the default user quota size? What is the default group quota size?</li><li>• Space utilization Do you want to guarantee space for data and Snapshot copies? Do you want to reserve space for Snapshot copies? (If so, the default is 20 percent of the total volume size. You can manually resize the Snapshot reserve space later.)</li></ul>
<b>SAN container properties</b>	<ul style="list-style-type: none"><li>• Type of container: Do you want dataset members to be provisioned in volumes or LUNs?</li><li>• Space settings:<ul style="list-style-type: none"><li>• Do you want to guarantee space for the container and Snapshot copies?</li><li>• Do you want to guarantee space for the container and automatically grow space for Snapshot copies on demand by preserving the existing Snapshot copies during write activity? This option requires more space.</li><li>• Do you want to guarantee space for the container and increase the space for Snapshot copies on demand by automatically deleting Snapshot copies when necessary? This option requires the storage systems to run Data ONTAP 7.2.4 or later. This is the default option.</li></ul></li></ul>

- Do you not want to guarantee space for the container or Snapshot copies?

**Space thresholds** Do you want to set threshold levels for space utilization and receive event notifications when those thresholds are reached? If so, at what percentage of the dataset maximum size do you want the following to occur:

- A Nearly Full threshold event warning message generated?
- A Full threshold event error message generated?

**Provisioning script** Do you want to use a custom provisioning script to perform tasks after storage is provisioned? If so, what is the full path of the script on the DataFabric Manager server?

**Note:** The licensed provisioning application only supports native executables or batch files (.bat, .cmd) on Windows. If you want to specify a backup script that is not in a native Windows language, you must enclose it inside a batch file.

## Next topics

[Types of provisioning policies](#) on page 863

[What storage availability levels are](#) on page 864

[What a resource label is](#) on page 867

[Space utilization thresholds](#) on page 872

[What provisioning scripts are](#) on page 873

## Related tasks

[Adding a provisioning policy](#) on page 875

## Related references

[Provisioning policy properties](#) on page 853

# Types of provisioning policies

A NAS provisioning policy can provision and export storage for NFS/CIFS access on a primary node; a SAN provisioning policy can provision and export storage for FCP/iSCSI access. If you also have a protection license, a provisioning policy can provision storage for backup and mirror destinations on a secondary node.

When you create a new provisioning policy, the policy settings describe the desired storage in terms of availability, performance, and exports. The policy settings also describe how the storage should be provisioned, exported, and managed.

Storage used for different purposes requires different sets of settings, so there is more than one type of provisioning policy you can create.

- |                  |   |
|------------------|---|
| <b>NAS</b>       | Choose the NAS provisioning policy type to provision storage that will be exported as NFS or CIFS shares. NAS provisioning policies also enable you to set default quotas for each user or UNIX group that writes data to the storage and to manage the space reserved for storing Snapshot copies. |
| <b>SAN</b>       | Choose the SAN provisioning policy type to provision storage to be accessed using FCP or iSCSI protocols. SAN provisioning policies also enable you to manage the space needed for Snapshot copies.   |
| <b>Secondary</b> | Choose the Secondary provisioning policy type to provision volumes for backups and mirror copies on the secondary nodes of a dataset. This policy type is available only when you have the Provisioning and Protection licenses.  |

## What storage availability levels are

You can select the level of availability of the storage resources that is required for datasets. When the licensed application uses a provisioning policy to provision datasets, it searches the resource pool for a storage resource that provides only the availability level specified and no higher.

The storage availability properties are related to various aggregate and storage controller configurations. The availability levels that datasets might require are as follows:

- Double disk failure  
The application looks for storage resources configured using RAID-DP aggregates to protect data from double disk failures. This is the default value.
- Single disk failure  
The application looks for storage resources configured using RAID4 aggregates to protect data from single disk failures. This option is the default if no reliability level is specified.  
**Note:** V-Series storage is assumed to be single-disk failure protection because some resiliency properties might not be detectable by the management console applications.
- Externally managed RAID  
RAID protection is determined by V-Series storage capabilities.
- Storage subsystem failure  
The application looks for storage resources using SyncMirror aggregates to protect data from failures of adapters, cables, and shelves.
- Storage controller failure  
The application looks for storage resources using an active/active configuration to protect data from controller failures.

**Note:** If the application does not find a resource that provides the specified availability level, then the provisioning request fails.

### Next topics

[What RAID4 protection is](#) on page 865

[What RAID-DP protection is](#) on page 865

## What RAID4 protection is

If an aggregate is configured for RAID4 protection, Data ONTAP reconstructs the data from a single failed disk within a RAID group and transfers that reconstructed data to a spare disk.

RAID4 provides single-parity disk protection against single-disk failure within a RAID group.

The minimum number of disks in a RAID4 group is two: at least one data disk and one parity disk.

If there is a single data or parity disk failure in a RAID4 group, Data ONTAP replaces the failed disk in the RAID group with a spare disk and uses the parity data to reconstruct the failed disk's data on the replacement disk. If no spare disks are available, Data ONTAP goes into degraded mode and alerts you of this condition.

**Attention:** With RAID4, if there is a second disk failure before data can be reconstructed from the data on the first failed disk, there will be data loss. To avoid data loss when two disks fail, you can select RAID-DP. This provides two parity disks to protect you from data loss when two disk failures occur in the same RAID group before the first failed disk can be reconstructed.

## What RAID-DP protection is

If an aggregate is configured for RAID-DP protection, Data ONTAP reconstructs the data from one or two failed disks within a RAID group and transfers that reconstructed data to one or two spare disks as necessary.

RAID-DP provides double-parity disk protection when the following conditions occur:

- There is a single-disk or double-disk failure within a RAID group.
- There are media errors on a block when Data ONTAP is attempting to reconstruct a failed disk.

The minimum number of disks in a RAID-DP group is three: at least one data disk, one regular parity disk, and one double-parity (or dParity) disk.

If there is a data-disk or parity-disk failure in a RAID-DP group, Data ONTAP replaces the failed disk in the RAID group with a spare disk and uses the parity data to reconstruct the data of the failed disk on the replacement disk. If there is a double-disk failure, Data ONTAP replaces the failed disks in the RAID group with two spare disks and uses the double-parity data to reconstruct the data of the failed disks on the replacement disks.

## What SyncMirror is

SyncMirror is an optional feature of Data ONTAP. It is used to mirror aggregates.

The SyncMirror software creates aggregates that consist of two copies of the same WAFL file system. The two copies, known as plexes, are simultaneously updated. Therefore, the copies are always identical.

For more information about aggregates and volumes, see the *Data ONTAP Storage Management Guide*.

### Related information

*Data ONTAP Storage Management Guide* -

[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

## Advantages of using SyncMirror

A SyncMirror relationship between two aggregates provides a high level of data availability because the two plexes are physically separated.

For a storage system using disks, the two plexes are on different shelves connected to the storage system with separate cables and adapters. Each plex has its own collection of spare disks. For a storage system using third-party storage, the plexes are on separate sets of array LUNs, either on one storage array or on separate storage arrays.

**Note:** You cannot set up SyncMirror with disks in one plex and array LUNs in the other plex.

Physical separation of the plexes protects against data loss if one of the shelves becomes unavailable. The unaffected plex continues to serve data while you fix the cause of the failure. Once fixed, the two plexes can be resynchronized and the mirror relationship reestablished.

Another advantage of mirrored plexes is faster rebuild time.

In contrast, if an aggregate using SnapMirror for replication becomes unavailable, you can use one of the following options to access the data on the SnapMirror destination (secondary).

- The SnapMirror destination cannot automatically take over the file serving functions. However, you can manually set the SnapMirror destination to allow read-write access to the data.
- You can restore the data from the SnapMirror destination to the primary (source) storage system .

The disadvantage of SyncMirror is that a mirrored aggregate requires twice as many disks as an unmirrored aggregate. Each of the two plexes requires a full set of disks. For example, you need 2,880 GB of disk space to mirror a 1,440-GB aggregate—1,440 GB for each plex of the mirrored aggregate.

## What an active/active configuration is

An active/active configuration is two storage systems (nodes) whose controllers are connected to each other either directly or through switches.

You can configure the active/active configuration so that each node in the pair shares access to a common set of storage, subnets, and tape drives, or each node can own its own distinct set of storage.

The nodes are connected to each other through a NVRAM adapter, or, in the case of systems with two controllers in a single chassis, through an internal interconnect. This allows one node to serve data to the disks of its failed partner node. Each node continually monitors its partner, mirroring the data for each other's nonvolatile memory (NVRAM or NVMMEM).

## Benefits of an active/active configuration

Active/active configurations provide fault tolerance and the ability to perform nondisruptive upgrades and maintenance. Configuring storage systems in an active/active configuration provides the following benefits:

- Fault tolerance  
When one node fails or becomes impaired a takeover occurs, and the partner node continues to serve the failed node's data.
- Nondisruptive software upgrades  
When you halt one node and allow takeover, the partner node continues to serve data for the halted node while you upgrade the node you halted.
- Nondisruptive hardware maintenance  
When you halt one node and allow takeover, the partner node continues to serve data for the halted node while you replace or repair hardware in the node you halted.

## What a resource label is

Resource labels act as filters. You can add an identifying label to storage resources and then configure a provisioning policy to provision storage only from resources that match that label.

When a provisioning policy is configured with a resource label, all provisioning requests using that policy are matched with available resources configured with the same resource label.

A resource label is a text string of any length.

Use resource labels sparingly because they restrict the amount of available resources from which additional storage can be provisioned. They are useful for targeting specific resources: for example, resources in a particular geographic area, or resources of a particular type, such as high-speed storage.

## Why you use quotas

You can use quotas to limit resource usage, to provide notification when resource usage reaches specific levels, or simply to track resource usage.

You specify a quota for the following reasons:

- To limit the amount of disk space or the number of files that can be used by a user or group, or that can be contained by a qtree
- To track the amount of disk space or the number of files used by a user, group, or qtree, without imposing a limit
- To warn users when their disk usage or file usage is high

## Overview of the quota process

Quotas can cause Data ONTAP to send a notification (soft quota) or to prevent a write operation from succeeding (hard quota) when quotas are exceeded.

When Data ONTAP receives a request to write to a volume, it checks to see whether quotas are activated for that volume. If so, Data ONTAP determines whether any quota for that volume (and, if the write is to a qtree, for that qtree) would be exceeded by performing the write operation. If any hard quota would be exceeded, the write operation fails, and a quota notification is sent. If any soft quota would be exceeded, the write operation succeeds, and a quota notification is sent.

## Quota targets and types

Quota targets determine whether a quota operates on a user, group, or qtree; targets determine the quota type.

Quota target	Quota type	How target is represented	Notes
user	user quota	UNIX user name UNIX UID A file or directory whose UID matches the user  Windows user name in pre-Windows 2000 format  Windows SID  A file or directory with an ACL owned by the user's SID	User quotas can be applied for a specific volume or qtree.

Quota target	Quota type	How target is represented	Notes
group	group quota	UNIX group name UNIX GID A file or directory whose GID matches the group	Group quotas can be applied for a specific volume or qtree. <b>Note:</b> Data ONTAP does not apply group quotas based on Windows IDs.
*	user group tree	The asterisk character (*)	A quota target of * denotes a <i>default quota</i> . For default quotas, the quota type is determined by the value of the type field.

## How space management works

The space management capabilities of Data ONTAP allow you to configure your storage systems to provide the storage availability required by the users and applications accessing the system, while using your available storage as effectively as possible.

Data ONTAP enables space management using the following capabilities:

- Space guarantees
- Space reservations
- Fractional reserve
- Automatic free space preservation

## What space guarantees are

Space guarantees on a FlexVol volume ensure that writes to a specified FlexVol volume or writes to files with space reservations enabled do not fail because of lack of available space in the containing aggregate.

Space guarantee is an attribute of the volume. It is persistent across storage system reboots, takeovers, and givebacks. Space guarantee values can be `volume` (the default value), `file`, or `none`.

- A space guarantee of `volume` reserves space in the aggregate for the volume. The reserved space cannot be allocated to any other volume in that aggregate.

The space management for a FlexVol volume that has a space guarantee of `volume` is equivalent to a traditional volume.

- A space guarantee of `file` reserves space in the aggregate so that any file in the volume with space reservation enabled can be completely rewritten, even if its blocks are being retained on disk by a Snapshot copy.
- A FlexVol volume that has a space guarantee of `none` reserves no extra space for user data; writes to LUNs or files contained by that volume could fail if the containing aggregate does not have enough available space to accommodate the write.

**Note:** Because out-of-space errors are unexpected in a CIFS environment, do not set space guarantee to `none` for volumes accessed using CIFS.

When space in the aggregate is reserved for space guarantee for an existing volume, that space is no longer considered free space. Operations that consume free space in the aggregate, such as creation of Snapshot copies or creation of new volumes in the containing aggregate, can occur only if there is enough available free space in that aggregate; these operations are prevented from using space already committed to another volume.

When the uncommitted space in an aggregate is exhausted, only writes to volumes or files in that aggregate with space guarantees are guaranteed to succeed.

**Note:** Space guarantees are honored only for online volumes. If you take a volume offline, any committed but unused space for that volume becomes available for other volumes in that aggregate. When you bring that volume back online, if there is not sufficient available space in the aggregate to fulfill its space guarantees, you must use the force (`-f`) option, and the volume's space guarantees are disabled. When a volume's space guarantee is disabled, the word `(disabled)` appears next to its space guarantees in the output of the `vol status` command.

## What space reservation is

When space reservation is enabled for one or more LUNs, Data ONTAP reserves enough space in the volume (traditional or FlexVol) so that writes to those LUNs do not fail because of a lack of disk space.

**Note:** LUNs in this context refer to the LUNs that Data ONTAP serves to clients, not to the array LUNs used for storage on a storage array.

For example, if you create a 100-GB space reserved LUN in a 500-GB volume, that 100 GB of space is immediately allocated, leaving 400 GB remaining in the volume. In contrast, if space reservation is disabled on the LUN, all 500 GB in the volume remain available until writes are made to the LUN.

Space reservation is an attribute of the LUN; it is persistent across storage system reboots, takeovers, and givebacks. Space reservation is enabled for new LUNs by default, but you can disable or enable it by using the `lun set reservation` command.

When a volume contains one or more LUNs with space reservation enabled, operations that require free space, such as the creation of Snapshot copies, are prevented from using the reserved space. If these operations do not have sufficient unreserved free space, they fail. However, writes to the LUNs with space reservation enabled will continue to succeed.

## Related information

*Technical Report: Thin Provisioning in a SAN or IP SAN Enterprise Environment -*  
<http://media.netapp.com/documents/tr3483.pdf>

# What fractional reserve is

If you have enabled space reservation, you can use the `vol options` command to set fractional reserve, which reduces the size of the reserved space in the volume.

Fractional reserve can be set to any percentage from zero to 100. However, you can only set fractional reserve to a non-zero value when you are not using the autodelete function.

It is generally recommended to use the autodelete function, but there may occasionally be circumstances under which fractional reserve can be used, including:

- When Snapshot copies cannot be deleted
- When preserving existing Snapshot copies is more important than creating new ones

Fractional reserve can be used on the following types of volumes:

- Traditional volumes
- FlexVol volumes with a space guarantee of `volume`

**Note:** If the `guarantee` option for a FlexVol volume is set to `file`, then fractional reserve for that volume is set to 100 percent and is not adjustable.

The default setting for fractional reserve is 100 percent. This means that when you create space-reserved LUNs, you can be sure that writes to those LUNs will always succeed without deleting Snapshot copies, even if all of the space-reserved LUNs are completely overwritten.

Setting fractional reserve to less than 100 percent causes the space reservation held for all space-reserved LUNs in that volume to be reduced to that percentage. Writes to the space-reserved LUNs in that volume are no longer unequivocally guaranteed.

Fractional reserve is generally used for volumes that hold LUNs with a small percentage of data overwrite.

**Note:** If you are using fractional reserve in environments in which write errors due to lack of available space are unexpected, you must monitor your free space and take corrective action to avoid write errors. Data ONTAP provides tools for monitoring available space in your volumes.

**Note:** Reducing the space reserved for overwrites (by using fractional reserve) does not affect the size of the space-reserved LUN. You can write data to the entire size of the LUN. The space reserved for overwrites is used only when the original data is overwritten.

### Example

If you create a 500-GB space-reserved LUN, then Data ONTAP ensures that 500 GB of free space always remains available for that LUN to handle writes to the LUN.

If you then set fractional reserve to 50 for the LUN's containing volume, then Data ONTAP reserves 250 GB, or half of the space it was previously reserving for overwrites with fractional reserve set to 100. If more than half of the LUN is overwritten, then subsequent writes to the LUN could fail due to insufficient free space in the volume.

**Note:** When more than one LUN in the same volume have space reservations enabled, and fractional reserve for that volume is set to less than 100 percent, Data ONTAP does not limit any space-reserved LUN to its percentage of the reserved space. In other words, if you have two 100-GB LUNs in the same volume with fractional reserve set to 30, one of the LUNs could use up the entire 60 GB of reserved space for that volume.

Refer to the Technical Report on thin provisioning below for more detailed information on using fractional reserve .

### Related information

*Technical Report: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment - <http://media.netapp.com/documents/tr3483.pdf>*

## Space utilization thresholds

Provisioning policies enable you to set thresholds indicating the points at which a dataset member is considered full or nearly full, such as a volume running out of space or a qtree running out of quota.

These thresholds are used to generate warning and error events and to compute the overall space status of the dataset.

**Nearly full** This threshold generates a warning event when the used space in a dataset member meets or exceeds a specified percentage. The setting for this threshold must be lower than the setting of the Full threshold to generate meaningful events. The default setting is 80%.

**Full** This threshold generates an error event when the used space in a dataset member meets or exceeds a specified percentage. The default setting is 90%.

You can enable or disable space utilization thresholds for the datasets to which a provisioning policy is applied by editing the policy properties.

## What provisioning scripts are

After the licensed application provisions storage for a dataset, you might want the application to automatically run a custom script that performs additional configuration operations on the newly provisioned storage.

For example, you might use a script to set advanced volume options (like flexshare priority or security style) or, if you are using an older version of SnapDrive with SAN datasets, to export the provisioned volume using CIFS. When processing a provisioning scripts, the licensed application exports all objects associated with containers in a dataset as ENV variables (volume, qtree, LUN names, storage system or aggregate name on which the containers reside, and CIFS or NFS export names).

For information on how to write and execute a custom script, see the *Operations Manager Administration Guide*.

### Related information

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)



# Adding a provisioning policy

---

Use the **Add Provisioning Policy** wizard to add new provisioning policies. After you create a provisioning policy, you can assign it to dataset nodes to automatically manage their provisioning.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the information available that you need to complete this task:

- Name of the policy (required)
- Storage type: NAS, SAN (required)
- Level of storage availability required (optional)
- Resource label (optional)
- Deduplication type and schedule (optional)
- NAS or SAN settings (required)
- Nearly Full and Full thresholds (optional)
- Provisioning script (optional)

## Steps

1. From the navigation pane, click **Policies > Provisioning**.
2. Click **Add** to start the **Add Provisioning Policy** wizard.
3. After you complete each property page in the wizard, click **Next**.
4. Confirm the details of the policy and click **Finish**.

## After you finish

Your new policy is listed in the **Provisioning Policies** window.

## Related concepts

[Decisions to make before adding a provisioning policy](#) on page 861

## Related tasks

[Enabling deduplication on your dataset nodes](#) on page 809

## Related references

[Provisioning policy properties](#) on page 853

[Administrator roles and capabilities](#) on page 1055



# Decisions to make before editing a provisioning policy

---

Before you modify a provisioning policy, you need to gather the information required to complete the Edit pages.

**General properties** You can modify the name and description but you cannot change the storage type.

**Storage availability properties** You can modify the level of reliability required by dataset members using this policy. (Only the specified availability is selected; storage with a higher level of availability will not be selected.) The choices are:

- RAID-DP (Double disk failure)  
The application provisions from storage resources that are configured using aggregate RAID-DP.
- RAID4 (Single disk failure)  
The application provisions from storage resources that are configured using aggregate RAID4.

**Note:** V-Series storage is assumed to be single-disk failure protection because some resiliency properties might not be detectable by the management console applications.

- Externally managed RAID  
The application provisions from V-Series storage. Therefore, RAID protection is determined by the V-Series storage capabilities.
- Storage subsystem failure (aggregate SyncMirror)  
The application provisions from storage resources that use aggregate SyncMirror.
- Storage controller failure (active/active configuration )  
The application provisions from storage resources that have an active/active configuration.

**Resource label (optional)** You can add or modify the resource label used to match provisioning requests with available resources.

**NAS container properties** You can modify the quota settings and the space utilization properties.

**SAN container properties** You can modify which container types to provision for datasets and the space utilization properties.

<b>Space thresholds</b>	You can modify the threshold levels for space utilization and whether you want to receive event notifications when those thresholds are reached.
<b>Provisioning script</b>	You can modify the name or the path of a provisioning script that is run after storage is provisioned.
<b>Preview</b>	You can use this page to test your modifications. The application displays a message describing the results of the test.
<b>Deduplication settings</b>	<p>Do you want data deduplication enabled on the volumes residing in the dataset node to which this provisioning policy is applied? If so, what kind of deduplication do you want to enable?</p> <ul style="list-style-type: none"><li>• Do you want only to run Manual deduplication? If you decide to configure this option, deduplication starts only when you manually select a volume and click the <b>Dedupe Now</b> button.</li><li>• Do you want enable Auto deduplication? If you decide to enable auto deduplication, deduplication automatically starts on a volume that resides on this dataset node when that volume contains 20% new data written to it since the last deduplication run.</li><li>• Do you want to attach a Custom schedule for deduplication? If you decide to schedule deduplication, you can specify deduplication to start on which days of the week, during what time period, at what frequency, and during that time period.</li></ul>

## Related tasks

[Editing a provisioning policy](#) on page 879

## Related references

[Provisioning policy properties](#) on page 853

# Editing a provisioning policy

---

You can edit a provisioning policy property by selecting it on the **Provisioning Policies** window and clicking Edit.

## Before you begin

- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.
- Confirm that the change you want to make to this provisioning policy is acceptable for all datasets currently using this policy.

## Steps

1. From the navigation pane, click **Policies > Provisioning**.
2. Click the Dependencies tab at the bottom of the window.
3. Select the provisioning policy that you want to modify and note the datasets that are dependent on that policy. If any of the dependent datasets will be negatively affected by the policy modification you plan to make, first unassign the policy from the dataset.
4. Click the Details tab.
5. Select the provisioning policy that you want to modify and click **Edit**.
6. In the **Properties** sheet for the selected policy, click the page for the properties you want to modify and enter the new property values.

At any time while in the **Properties** sheet, you can click the Preview page to see an updated summary of your changes before they are applied.

7. When you are finished, do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the window.
  - Click **Cancel** to discard the changes you have made to the current policy.

## Related concepts

[Decisions to make before editing a provisioning policy](#) on page 877

## Related tasks

[Enabling deduplication on your dataset nodes](#) on page 809

[Disabling deduplication on dataset nodes](#) on page 811

## Related references

[Provisioning policy properties](#) on page 853

*Administrator roles and capabilities* on page 1055

# Copying a provisioning policy

---

Instead of creating a completely new provisioning policy, you can make a copy of a provisioning policy and modify it.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies** ▶ **Provisioning** Overview tab.
2. Select the provisioning policy that most closely resembles the policy you want to add and click **Copy**.  
The new policy is added to the list with the name "Copy of *policy-name*".
3. Select the new copy and click **Edit**.
4. In the **Properties** sheet, click the tab for the properties you want to modify and enter the new property values.
5. When you are finished, do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current policy.
  - Click **OK** to apply your changes and close the window.
  - Click **Cancel** to discard the changes you have made to the current policy.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a provisioning policy

---

You can delete an existing provisioning policy if that policy is not currently applied to any dataset.

## Before you begin

- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.
- Make sure that each provisioning policy you want to delete is no longer assigned to any existing storage sets.

## Steps

1. From the navigation pane, click **Policies > Provisioning**.
2. Click the Dependencies tab at the bottom of the window.
3. Select a provisioning policy that you want to delete and confirm in the dependencies list that there are no datasets dependent on that policy.
4. If a selected policy has dependent dataset members, click **Data > Datasets > Overview** and assign another provisioning policy to the dependent dataset members.  
The dependencies list for the provisioning policy must be empty before you continue to the next step.
5. Click the Details tab in the **Provisioning Policies** window.
6. Select one or more provisioning policies that you want to delete and click **Delete**.

**Note:** The Delete button is not enabled for policies that are still attached to datasets.

7. Click **OK** in the confirmation dialog box to delete the selected policy, or click **Cancel** to cancel the delete request.

The selected policy is deleted from the policies list.

## Related references

[Administrator roles and capabilities](#) on page 1055



# What vFiler templates are

---

A vFiler template is a set of vFiler configuration settings, including the corresponding CIFS, DNS, NIS, and administrative host configuration settings, that you want to use as default settings for one or more vFiler units that you plan to add as hosts. You can configure as many vFiler templates as you need.

When adding a vFiler unit as a host, you can specify a vFiler template that provides the default configuration settings for that vFiler unit. In addition to the configuration settings provided by the vFiler template, you also must specify those values that are unique to the vFiler unit, such as name and IP address.

## Related concepts

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

[\*Decisions to make before adding vFiler templates\*](#) on page 891



# vFiler template properties

---

With certain exceptions and caveats, you can specify, view, and modify property values to suit your needs.

You can specify, view, and modify property values as follows:

- You can provide a value for a property in the **Add vFiler Template** wizard.
- You can view a property in the **vFiler Templates** window.
- You can modify a property in the **Properties** sheet, which is accessed by clicking **Edit** in the **vFiler Templates** window.

You can specify, view, or modify the following vFiler template attributes:

<b>Name</b>	The name assigned to a vFiler template. Name is a required property.  Special characters and spaces are permitted in names. The limit is 64 characters, but for readability, you should keep the name under 25 characters.				
<b>Description</b>	A description of the vFiler template. It might include the intended use of the vFiler template or some other common attribute that identifies why the vFiler template was created. Description is an optional property.				
<b>Administrative Host</b>	The IP address of the host that has root access to the files needed for system administration for a vFiler unit using the selected vFiler template. Administrative Host is an optional property.				
<b>DNS domain</b>	<table> <tr> <td><b>Name</b></td><td>The name of the DNS domain to which a vFiler unit using the selected vFiler template belongs. DNS domain is a required property.</td></tr> <tr> <td><b>Servers</b></td><td>The IP addresses of the DNS domain servers. Domain server is a required property.</td></tr> </table>	<b>Name</b>	The name of the DNS domain to which a vFiler unit using the selected vFiler template belongs. DNS domain is a required property.	<b>Servers</b>	The IP addresses of the DNS domain servers. Domain server is a required property.
<b>Name</b>	The name of the DNS domain to which a vFiler unit using the selected vFiler template belongs. DNS domain is a required property.				
<b>Servers</b>	The IP addresses of the DNS domain servers. Domain server is a required property.				
<b>NIS domain</b>	<table> <tr> <td><b>Name</b></td><td>The name of the NIS domain to which a vFiler unit using the selected vFiler template belongs. NIS domain is a required property.</td></tr> <tr> <td><b>Servers</b></td><td>The IP addresses of the NIS domain servers. Domain server is a required property.</td></tr> </table>	<b>Name</b>	The name of the NIS domain to which a vFiler unit using the selected vFiler template belongs. NIS domain is a required property.	<b>Servers</b>	The IP addresses of the NIS domain servers. Domain server is a required property.
<b>Name</b>	The name of the NIS domain to which a vFiler unit using the selected vFiler template belongs. NIS domain is a required property.				
<b>Servers</b>	The IP addresses of the NIS domain servers. Domain server is a required property.				
<b>CIFS Settings</b>	<table> <tr> <td><b>Security protocol</b></td><td>The security protocol to be used by a vFiler unit using this vFiler template. This is a required property only for CIFS protocol users. Valid values are NTFS-only and Multiprotocol.</td></tr> </table>	<b>Security protocol</b>	The security protocol to be used by a vFiler unit using this vFiler template. This is a required property only for CIFS protocol users. Valid values are NTFS-only and Multiprotocol.		
<b>Security protocol</b>	The security protocol to be used by a vFiler unit using this vFiler template. This is a required property only for CIFS protocol users. Valid values are NTFS-only and Multiprotocol.				

<b>Authentication mode</b>	Authentication type used by CIFS clients. This is a required property only for CIFS protocol users. Valid values are Active Directory and Windows Workgroup.
<b>Domain name</b>	The name of the CIFS domain to which a vFiler unit using the selected vFiler template belongs. This is a required property only for CIFS protocol users when the authentication mode is active directory.

#### Related concepts

*[Decisions to make before adding vFiler templates](#)* on page 891

#### Related tasks

*[Adding a vFiler template](#)* on page 893

*[Editing a vFiler template](#)* on page 895

# Viewing vFiler templates

---

You can view all the vFiler templates and their properties on the **vFiler Templates** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Step

1. From the navigation pane, click **Policies > vFiler Templates**.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Decisions to make before adding vFiler templates

---

Before you start the **Add vFiler Template** wizard, you need to gather the information required to complete the wizard.

**Name and description** What name do you want to use for the new template? Do you want to add a description? Descriptions are helpful when you need to select the appropriate vFiler template when you are adding a vFiler host.

**Administrative host** What is the address of the administrative host that will be used by all vFiler hosts to which this template is assigned?

**DNS domain settings** If vFiler hosts using this template will use DNS protocol, gather the following information:

- What is the domain name?
- What are the addresses of the domain servers?

**NIS domain settings** If vFiler hosts using this template will use NIS protocol, gather the following information:

- What is the domain name?
- What are the addresses of the domain servers?

**CIFS settings** If vFiler hosts using this template will use CIFS protocol, gather the following information:

- Security protocol: Will the vFiler host use NTFS-only or will it use other protocols (multiprotocol)?
- Authentication mode: What is the authentication mode that will be used: the active directory or the Windows workgroup?
- What is the domain name? By default, the CIFS domain name is the same as the DNS domain name that you entered.

## Related concepts

[What vFiler templates are](#) on page 885

## Related tasks

[Adding a vFiler template](#) on page 893

**Related references**

[\*vFiler template properties\*](#) on page 887

# Adding a vFiler template

---

You can use the **Add vFiler Template** wizard to create and add new vFiler templates. After you create a vFiler template, you can apply it to vFiler hosts to automatically configure them with the default settings specified in the template.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > vFiler Templates**.
2. Click **Add** to start the **Add vFiler Template** wizard.
3. After you complete each property sheet in the wizard, click **Next**.
4. Confirm the details of the policy and click **Finish**.

Your new policy is listed in the **vFiler Templates** window.

## Related concepts

*Decisions to make before adding vFiler templates* on page 891

## Related references

*vFiler template properties* on page 887

*Administrator roles and capabilities* on page 1055



# Editing a vFiler template

---

You can edit a vFiler template property by selecting it on the **vFiler Templates** window and clicking **Edit**.

## Before you begin

- Confirm that the change that you want to make to this vFiler template is acceptable for all vFiler units that are using this policy.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > vFiler Templates**.
2. Select the vFiler template that you want to modify and click **Edit**.
3. In the **Properties** sheet for the selected template, click the tab for the properties that you want to modify and enter the new property values.
4. When you are finished, do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current template.
  - Click **OK** to apply your changes and close the window.

## Related references

[vFiler template properties](#) on page 887

[Administrator roles and capabilities](#) on page 1055



# Copying a vFiler template

---

You can make a copy of a vFiler template and modify it rather than creating a completely new vFiler template.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies > vFiler Templates**.
2. Select the vFiler template that most closely resembles the template that you want to add and click **Copy**.  
The new template is added to the list with the name *Copy of template-name*.
3. Select the new copy and click **Edit**.
4. In the **Properties** sheet, click the tab for the properties that you want to modify and enter the new property values, including a new name.
5. When you are finished, do one of the following:
  - Click **Apply** to apply your changes and continue to edit the current template.
  - Click **OK** to apply your changes and close the window.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Deleting a vFiler template

---

You can delete an existing vFiler template if that template is not currently applied to an existing dataset.

## Before you begin

- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.
- Make sure that the vFiler template that you want to delete is no longer assigned to any storage sets.

## Steps

1. From the navigation pane, click the **Policies > vFiler Templates** tab.
2. Select one or more vFiler templates that you want to delete.
3. Click **Delete**, then click **OK** in the confirmation dialog box to delete the selected policy or click **Cancel** to cancel the delete request.

The selected template is deleted from the vFiler template list.

## Related references

[Administrator roles and capabilities](#) on page 1055



# How hosts become visible to the console

---

The hosts that you can view in NetApp Management Console and use in your policy implementations have been automatically discovered by DataFabric Manager or manually added to its database.

## Host discovery

When either Protection Manager or Provisioning Manager is enabled, DataFabric Manager automatically begins a host discovery process. The discovered hosts automatically display in the lists of storage system, vFiler unit, and Open Systems SnapVault client hosts in the provisioning and protection application interface.

When you add a host to NetApp Management Console, the host is incorporated into the DataFabric Manager database and is viewable in Operations Manager. You can add host systems in the management console from the **Storage Systems Hosts** window, **vFiler Units** window, and Open Systems SnapVault window.

Some items that are viewable as hosts in Operations Manager are not listed as hosts in the NetApp Management Console interface, because the console does not use items of that type to implement its data management tasks. For example, Fibre Channel switches are considered hosts in Operations Manager but are not included in the list of hosts in NetApp Management Console.

## Host monitoring

You can verify that a host is available and correctly configured by accessing the list in the appropriate Hosts window for storage systems, vFiler units, and Open Systems SnapVault systems. The protection and provisioning applications regularly check for updates to configuration information. This data is gathered from SNMP queries by system monitors. The monitors update the DataFabric Manager database at scheduled intervals. The protection and provisioning applications query the DataFabric Manager database for the information that is then displayed in NetApp Management Console.

Because the protection and provisioning applications do not query the hosts directly but rely on the scheduled monitors, the configuration information displayed in the Hosts windows is not real-time data. Therefore, this data might not reflect recent changes made to a storage system or configuration and could be outdated by a few minutes or a few hours, depending on the changes made.

For more information about host discovery and management with the DataFabric Manager database, see the *Operations Manager Administration Guide*.

## Related concepts

[Hosts that contain unprotected data](#) on page 439

## Related tasks

[How do I back up data?](#) on page 589

**Related information**

*Operations Manager Administration Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## Ways to investigate problems with hosts

---

If you are investigating a policy failure, you can use the information displayed in the Hosts windows to determine whether the cause is a problem with a host. This information can also help determine the potential impact of any changes that you might make to a host.

Most problems that you might encounter with a host can be diagnosed and corrected by using the host diagnostics wizards. The diagnostics wizards are located on the **Storage Systems Hosts** window and the **OSSV Hosts** window. The wizards include steps to help you locate and fix issues with hosts. You can also use the Edit hosts property sheets to make changes to host licenses and host and NDMP credentials. You can access each of the wizards and property sheets in the following windows of the interface.

**Storage Systems Hosts window** Provides information about storage systems that can help you verify whether a host is up and accepting the NDMP credentials specified for it, as well as whether the appropriate licenses are assigned to it.

Allows you to review path and relationship information about storage systems, as well as to check host and NDMP status. The path and relationship information displayed for each individually selected storage system helps you see the interdependencies between hosts. For example, by reviewing the data flowing into and out of a selected storage system, you can evaluate the impact of temporarily removing that storage system from service for maintenance. You can also review information about input and output relationships to determine whether lag times are within specified thresholds and which datasets are impacted if the lag threshold has been or is about to be exceeded.

From this window, you can start the **Add Storage System** wizard and the **Diagnose Storage Systems** wizard, or you can open the Edit property sheet for storage systems. You can also refresh the information about a selected host in the window's host list.

**vFiler Units window** Allows you to review the status of vFiler units and to verify the IP address of the vFiler unit and the name of the storage system that is hosting it.

Allows you to review path and relationship information about vFiler units. The path and relationship information displayed for each individually selected vFiler unit helps you see the interdependencies between hosts and datasets. For example, by reviewing the data flowing into and out of a selected host, you can evaluate the impact of temporarily removing that host from service for maintenance.

From this window, you can start the Add vFiler Unit wizard or the Setup vFiler Unit wizard, and you can delete vFiler units.

<b>OSSV Hosts window</b>	<p>Allows you to review the status of Open Systems SnapVault hosts (including VMware ESX hosts) the port and credentials status of each NetApp Host Agent , and the status of NDMP connections and credentials.</p>
	<p>Allows you to investigate problems with an Open Systems SnapVault client. Information in this window includes the host and NDMP status, the NDMP credentials status, the operating system and version that each host is running, and path information for each host.</p>

From this window, you can start the **Add OSSV Host** wizard and the **Diagnose OSSV Host** wizard, and open the Edit OSSV host property sheet for a host that contains an Open Systems SnapVault agent.

From this window, you can also stop and start an Open Systems SnapVault 2.3 and later agent on which NetApp Host Agent is installed. Stopping and starting the agent stops and starts backup service on the selected client, which might resolve the problem. After you restart the backup service, you can click **Refresh** to display current data for the selected client and determine the effect of restarting the backup service.

**Note:** There is no Open Systems SnapVault plugin for Solaris, so the NetApp Host Agent cannot talk to the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the NetApp Management Console .

## Related tasks

[Diagnosing a storage system](#) on page 947

[Diagnosing an Open Systems SnapVault host](#) on page 949

# Data ONTAP licenses used for protecting or provisioning data

---

There are several Data ONTAP licensed options that you can use to protect or provision your data. After you have purchased the software licenses you need, you can assign these licenses to your primary and secondary storage from the **Storage Systems Hosts** window.

When you purchase a Data ONTAP option license, you receive a code composed of a string of characters, such as ABCDEFG, that is unique to a particular service. You receive license codes for every protocol and option, or service, that you purchase.

Not all purchased license codes are installed on a storage system before it is shipped from the factory. Some licenses are installed after the system is set up. You can purchase license codes to enable additional services at any time. If you misplace a license code, you can contact NetApp technical support or log in to the NOW site to obtain a copy.

You must enter a software license code on a storage system to enable the corresponding service. You do not need to indicate which license the code enables. The code is matched automatically to the appropriate service license.

**Note:** The Licenses area is visible only when the selected host is a single storage system running Data ONTAP. If you plan to use Open Systems SnapVault to back up data on a host that is not running Data ONTAP, you select the secondary storage system to license the necessary Data ONTAP services.

The licenses available for use with Data Manager are:

**SnapMirror license** You install a SnapMirror license on each of the source and destination storage systems for the mirrored data. If the source and destination volumes are on the same system, only one license is required.

SnapMirror replicates data to one or more networked storage systems. SnapMirror updates the mirrored data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on nonproduction systems, online data migration, and so on. You can also enable the SnapMirror license to use Qtree SnapMirror for backup.

To use SnapMirror software, you must update the `snapmirror.access` option in Data ONTAP to specify the destination systems that are allowed to access the primary data source system. For more information about the `snapmirror.access` option, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

**SnapVaultData ONTAP secondary license** You install the SnapVault Secondary license on storage systems hosting the backups of protected data. SnapVault creates backups of data stored on multiple primary storage systems and copies the backups to a secondary storage system. If data loss or corruption occurs, backed-up data can be restored to a primary

	<p>or open storage system with little of the downtime and uncertainty associated with conventional tape backup and restore operations.</p>
<b>SnapVaultData ONTAP primary license</b>	<p>You install the SnapVaultData ONTAP Primary license on storage systems running Data ONTAP that contain host data to be backed up.</p>
<b>SnapVault Windows Primary License</b>	<p>You install the SnapVault Windows Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a Windows-based primary storage system running the Open Systems SnapVault agent. A Windows-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>SnapVault Windows Open File Manager license</b>	<p>You install the SnapVault Open File Manager license on a secondary storage system to enable the backup of open files on Windows primary storage systems running the Open Systems SnapVault agent.</p> <p>You must install the SnapVault Windows Primary license and the SnapVaultData ONTAP Secondary license on the secondary storage system before installing the SnapVault Open File Manager license.</p>
<b>SnapVault UNIX primary license</b>	<p>You install the SnapVault UNIX Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a UNIX-based primary storage system (AIX, HP-UX, or Solaris) running the Open Systems SnapVault agent. A UNIX-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>SnapVault Linux primary license</b>	<p>You install the SnapVault Linux Primary license on a secondary storage system, in addition to the SnapVault Secondary license, to support a Linux-based primary storage system running the Open Systems SnapVault agent. A Linux-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.</p>
<b>NearStore Option license</b>	<p>The NearStore license enables your storage system to use transfer resources as conservatively as if it were optimized as a backup system. This approach is useful when the storage system on which you want to store backed-up data is not a system optimized for storing backups, and you want to minimize the number of transfer resources the storage system requires.</p> <p>Storage systems using the NearStore license must meet the following criteria:</p> <ul style="list-style-type: none"><li>• The storage system must be a FAS30xx , FAS31xx series , or FAS60xx system.</li><li>• The version of Data ONTAP software must be 7.1 or later.</li><li>• If you plan to use the SnapVault service, the storage system must have a SnapVault secondary license enabled.</li></ul>

<b>Deduplication license</b>	The deduplication license enables you to consolidate blocks of duplicate data into single blocks to store more information using less storage space.
<b>SnapMirror Sync license</b>	The SnapMirror Sync license enables you to replicate data to the destination as soon as it is written to the source volume. SnapMirror Sync is a feature of SnapMirror.
<b>MultiStore Option license</b>	<p>The MultiStore Option license enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems on the network. Each virtual "storage system" created as a result of the partitioning is called a vFiler unit. A vFiler unit, using the resources assigned, delivers file services to its clients as a storage system does.</p> <p>The storage resource assigned to a vFiler unit can be one or more qtrees or volumes. The storage system on which you create vFiler units is called the hosting storage system. The storage and network resources used by the vFiler units exist on the hosting storage system.</p> <p>Be sure the host on which you intend to install the MultiStore Option license is running Data ONTAP version 6.5 or later.</p>

## Related concepts

[When qtree SnapMirror is used to perform backups](#) on page 909

## Related tasks

[Adding a resource pool](#) on page 841

## Related information

[Data ONTAP Data Protection Tape Backup and Recovery Guide -](#)  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)



# **When qtree SnapMirror is used to perform backups**

The licensed protection application can use either SnapVault or qtree SnapMirror to perform backups. The protection application determines which technology to use based on the licenses enabled on the source and destination hosts and the schedule applied to the backup connection of the protection policy.

If you use only SnapVault licenses in your environment, the protection application uses SnapVault for backups. However, if you use both SnapVault and SnapMirror licenses in your environment, the protection application uses the following sequence to determine whether to use SnapVault or qtree SnapMirror for backups:

1. If the data to be backed up is located on a host running the Open Systems SnapVault agent, the protection application uses SnapVault for backups.
2. If either the source or destination host has the SnapMirror license enabled but not the SnapVault license, the protection application uses qtree SnapMirror for backups.
3. If both the source and destination host have the SnapVault license enabled but not the SnapMirror license, the protection application uses SnapVault for backups.
4. If the schedule applied to the backup connection specifies that the data needs to be backed up more frequently than once an hour, the protection application uses qtree SnapMirror for backups.
5. If none of the previous conditions applies, by default, the protection application uses SnapVault for backups.

## **Related references**

*[Data ONTAP licenses used for protecting or provisioning data](#)* on page 905



## How to customize a vFiler unit configuration using a script

---

You can write a script to customize a vFiler unit configuration. When the script is specified in the **Setup vFiler Unit** wizard, the licensed provisioning application executes the script before and after a vFiler unit is set up. You must specify the full DataFabric Manager server path of the script.

For example, if you want the new vFiler unit to use a vFiler unit configuration that was saved in Operations Manager, you might write a script that runs the appropriate `dfm config` commands to retrieve and execute that configuration.

For information on the environment variables you may need for a script, see the `dfpm` man pages in Operations Manager.



# Decisions to make before adding a storage system

Before running the **Add Storage System** wizard, it is useful to have all of the configuration information available for the host that you are adding.

**Host Name or IP Address** What is the name or the IP address of the storage system that you want to add?

**Licenses** Which services do you want enabled on the storage system?

You must enter a software license code to enable each corresponding service on the storage or host. Licenses are set immediately upon entering the information in the text field. License information cannot be removed or cancelled once entered, so be sure you are entering the correct storage system.

When you enable licenses, consider how you want to use each storage system to protect data:

- Can it be used to hold primary data or secondary data or both?
- Can it be used for backups or for mirroring?
- What operating system can it run on?

**Login Credentials** What are the user name and password for the storage system?

**Access Control** What roles do you want to have access privileges to the storage system?

You can assign different access privileges for SnapVault and for SnapMirror.

**NDMP Credentials** What is the NDMP user name for the storage system that you want to add?

DataFabric Manager automatically manages the password based on the user name provided. DataFabric Manager uses these credentials to communicate with the selected host over NDMP.

To obtain an encrypted NDMP password for a storage system, issue `ndmpd password username` from the command line of the storage system.

For more information about how Operations Manager uses NDMP, see the *Data ONTAP Storage Management Guide*. For more information about NDMP credentials, see the *Data ONTAP Data Protection Tape Backup and Recovery Guide*.

## Related tasks

[Adding a storage system](#) on page 915

**Related information**

*Data ONTAP Storage Management Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

*Data ONTAP Data Protection Tape Backup and Recovery Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

# Adding a storage system

---

You can add storage systems to the hosts list to make them available for inclusion in data management actions. When you add storage systems to NetApp Management Console, you also add the storage to the DataFabric Manager database.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available for the storage system that you want to add:

- Host name or IP address
- Host credentials (user name and password)
- License code
- SnapVault Access Control List, if licensed for SnapVault
- SnapMirror Access Control List, if licensed for SnapMirror
- NDMP credentials (user name and password)

## Steps

1. From the navigation pane, click **Hosts ▶ Storage Systems**.
2. Click **Add** to start the **Add Storage System** wizard.

Enter or select information as requested in the wizard.

**Note:** In this wizard, clicking Next implements the operations on each page. Clicking Back or Cancel does not undo operations performed on previous pages.

3. Verify that the storage system that you added is included in the hosts list in the **Storage Systems Hosts** window.

You might need to update the window before you can view the new host in the host list.

You can now manage data located on the new storage system or use the storage as a secondary storage system for backups or mirror copies.

## Related concepts

[Decisions to make before adding a storage system](#) on page 913

**Related tasks**

*How do I back up data?* on page 589

**Related references**

*Administrator roles and capabilities* on page 1055

# Decisions to make before adding an Open Systems SnapVault host

---

Before adding an Open Systems SnapVault host using the **Add OSSV Host** wizard, it is useful to have all of the host's configuration information available.

If the Open Systems SnapVault host you are adding resides on a VMwareESX 3.5 server, you should review the guidelines for adding an Open Systems SnapVault host on an ESX 3.5server.

**Host Name or IP Address** What is the name or the IP address of the Open Systems SnapVault host that you want to add?

**Host Agent Credentials**

- What are the user name and password that DataFabric Manager should use to authenticate to the host running NetApp Host Agent ?  
Operating system credentials for the host on which NetApp Host Agent is running, if DataFabric Manager is managing the credentials for you  
Credentials for NetApp Host Agent , if DataFabric Manager is NOT managing the credentials
- Should DataFabric Manager set up and manage the host agent password or will you do it manually?  
For instructions describing how to set up credentials for hosts running NetApp Host Agent , see the *NetApp Host Agent Installation and Administration Guide* .

**NetApp Host Agent Port** What port number do you want to use for host agent access?  
The default port is 4092.

**NDMP Credentials** What are the NDMP user name, password, and port number for the host that you want to add?  
DataFabric Manager uses these credentials to communicate with the selected host over NDMP.

To obtain an encrypted NDMP password for the host, issue `ndmpd password username` from the command line.

The default port number is 10000.

If the host runs the Open Systems SnapVault agent, specify the port number, if other than the default, that DataFabric Manager should use when communicating with the selected host over NDMP.

For more information about how Operations Manager uses NDMP, see the *Data ONTAP Storage Management Guide* . For more information about NDMP

credentials, see the *Data ONTAP Data Protection Tape Backup and Recovery Guide*.

For more information about Open Systems SnapVault configurations, see the *Open Systems SnapVault Installation and Administration Guide*.

#### **Related tasks**

[Adding an Open Systems SnapVault host](#) on page 921

#### **Related references**

[Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#) on page 919

#### **Related information**

*Open Systems SnapVault Installation and Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/client\\_filer\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/client_filer_index.shtml)

*Data ONTAP Storage Management Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

*Data ONTAP Data Protection Tape Backup and Recovery Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

# Guidelines for adding and editing an Open Systems SnapVault host on an ESX server

---

NetApp Management Console supports Open Systems SnapVault backups for virtual machines (VMs) on VMware ESX servers. Before starting the **Add OSSV Host** wizard for VMware ESX 3.5, it is useful to review the following guidelines.

- The Open Systems SnapVault software must be installed on each VMware ESX 3.5 server that you want to back up.
- The NetApp Host Agent is NOT needed for an Open Systems SnapVault installation on a VMware ESX 3.5 server.
- DataFabric Manager discovers only the virtual machines that are registered to the VMware ESX 3.5 server that you have discovered.
- NetApp Management Console backs up only the virtual machines on an VMware ESX 3.5 server. File system backups on a VMware ESX 3.5 server are not supported.
- The backup for the virtual machine is always through the VMware ESX 3.5 server that was involved in creating the relationship.

If the virtual machine is moved to another server, the backup is still through the original VMware ESX 3.5 server. If the original VMware ESX 3.5 server is offline, the virtual machine is not backed up.

For more information about Open Systems SnapVault configurations, see the *Open Systems SnapVault Installation and Administration Guide*.

## Related concepts

[Decisions to make before adding an Open Systems SnapVault host](#) on page 917

## Related tasks

[Adding an Open Systems SnapVault host](#) on page 921

[Editing Open Systems SnapVault properties](#) on page 939

[How do I back up data?](#) on page 589

## Related information

[Open Systems SnapVault Installation and Administration Guide - http://now.netapp.com/NOW/knowledge/docs/client\\_filer\\_index.shtml](#)



# Adding an Open Systems SnapVault host

---

You can add an Open Systems SnapVault host to make the host available to Data Manager for inclusion in data management actions. When you add an Open Systems SnapVault host to Data Manager, you also add the host to the DataFabric Manager database.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If the Open Systems SnapVault host you are adding resides on a VMware ESX 3.5 server, review the guidelines for adding an Open Systems SnapVault host on a VMware ESX 3.5 server.

Have the following information available for the host that you want to add:

- Host name or IP address
- Port number for NetApp Host Agent
- Decision about whether DataFabric Manager should set up and manage the NetApp Host Agent password:
  - If yes, provide the operating system credentials for the host on which NetApp Host Agent is running.
  - If no, provide the credentials for NetApp Host Agent .
- NDMP credentials (user name and password) and port number

## Steps

1. From the navigation pane, click **Hosts > OSSV** .
2. Click **Add** to start the **Add OSSV Host** wizard. Enter or select information as requested in the wizard.
3. Verify that the host you added is included in the hosts list in the **OSSV Hosts** window.

You might need to refresh the window before you can view the new host in the host list.

## Related concepts

[Decisions to make before adding an Open Systems SnapVault host](#) on page 917

## Related tasks

[How do I back up data?](#) on page 589

### Related references

- [Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#)* on page 919
- [Administrator roles and capabilities](#)* on page 1055

## Decisions to make before adding a vFiler unit

---

Before starting the **Add vFiler Unit** wizard, it is useful to have all of the following configuration information available for the unit that are you adding.

<b>Name</b>	What is the name of the vFiler unit that you want to add?  The vFiler unit name must be unique to that vFiler unit.
<b>IP space</b>	What is the IP space for the vFiler unit that you want to add?  An IP space defines an address in which the vFiler unit can participate. If no IP space is defined for the vFiler unit, use default-ipspace. For more information about vFiler IP space, see the <i>Data ONTAP MultiStore Management Guide</i> .
<b>Allowed protocols</b>	What protocols are assigned to the vFiler unit?  The following protocols are supported: <ul style="list-style-type: none"><li>• iSCSI</li><li>• NFS</li><li>• CIFS</li></ul> Fibre Channel is not supported on vFiler units.  <b>Attention:</b> If you assign the CIFS protocol to the vFiler unit, you need to set up CIFS before you can use the vFiler unit. Performing the setup stops and restarts CIFS, interrupting the CIFS service.
<b>Parent storage system or resource pool</b>	What storage system or resource pool is the vFiler unit assigned to?  Be sure the host on which you want to create a vFiler unit is running Data ONTAP version 7.0 or later.
<b>IP address</b>	What is the IP address of the vFiler unit that you want to add?  The IP address used by the vFiler unit must not be configured for use before you create the vFiler unit.  <b>Note:</b> The IP address accepts both IPv4 and IPv6 address formats.
<b>Network mask</b>	What is the network mask of the vFiler unit that you want to add?  The Network mask is not required to create the vFiler unit, although you must specify a network mask in order to setup the vFiler unit.

**Network interface** What is the Ethernet interface for the vFiler unit?

The Ethernet interface is not required to create the vFiler unit, although you must specify an interface before you can use the vFiler unit. If you plan to run scripts on the vFiler unit, you might choose to wait to specify the Ethernet interface later, by using the Setup option.

**VLAN ID** Will you use VLANs in the creation of the vFiler unit? What is the ID of the VLAN that you will use?

VLANs allow you to partition a physical network into multiple virtual networks that are totally separate from one another.

If the vFiler unit that you plan to add is created on an active/active host, you can use an existing VLAN ID or create a new VLAN ID for the vFiler unit. If a VLAN ID is not entered, the Partner interface field is disabled.

**Partner interface** What is the partner interface for the vFiler unit?

If you create a vFiler unit using an active/active host, the partner interface is selected automatically. If no partner interface is configured, then the option None is selected automatically.

The storage system on which the vFiler unit is created needs to be configured as an active/active configuration before the creation of the vFiler unit.

**vFiler template** Which, if any, vFiler template do you want to use for the vFiler unit?

A vFiler template is a set of vFiler configuration settings and the corresponding CIFS configuration settings. If you do not select a vFiler template, the network settings are cleared.

**CIFS workgroup name** What is the Windows workgroup name for the CIFS setup?

The Windows workgroup name specifies the name of the shared resources. The workgroup name option is displayed if the following apply:

- You select to use the CIFS protocol
- You select the Perform CIFS setup option
- You do not select a vFiler template or the template you select does not include CIFS settings

If you set up the vFiler unit to use the CIFS protocol, the vFiler units can use the same computer names as the servers. This enables CIFS clients to share resources without having to remap their drives or search for the new server.

<b>CIFS domain user and domain password</b>	What is the login name and the password for administrative access to the Active Directory system?  The domain user and domain password options are displayed if the following apply:
	<ul style="list-style-type: none"><li>• You select to use the CIFS protocol</li><li>• You select the Perform CIFS setup option</li><li>• You select a vFiler template that specifies Active Directory for CIFS authentication</li></ul>
<b>Root password</b>	What password will you use for the vFiler unit you are creating?

**Script path** Do you want to use a custom script to help manage vFiler units? If so, what is the full path of the script?

You can use the script while creating or setting up the vFiler unit.

**Note:** If the DataFabric Manager server is running on Windows, and if the post-setup script for the vFiler unit is on a network share, the script location must be specified by the full UNC path (no drive letter mapping).

## Related concepts

[What vFiler templates are](#) on page 885

[Considerations for active/active hosts](#) on page 933

## Related tasks

[Adding a vFiler unit](#) on page 927

## Related information

*Data ONTAP MultiStore Management Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)



# Adding a vFiler unit

---

You can create and configure vFiler units to make them available for inclusion in data management actions.

## Before you begin

Ensure that the host on which you want to create a vFiler unit is running Data ONTAP version 7.0 or later.

Ensure that the IP address used by the vFiler unit is not configured when you create the vFiler unit.

Have the following information available for the vFiler unit that you want to create:

- Name
- IP space
- Protocols assigned to the vFiler unit (NFS, CIFS, iSCSI)
- IP address
- Name of the storage system or resource pool to be associated with the vFiler unit
- Network mask
- Network interface to use
- VLAN id information (optional in an active/active configuration)
- Partner interface in an active/active configuration (disabled if VLAN id is not provided)
- vFiler template name (optional)
- Windows workgroup name or the CIFS domain user and password
- Root password (optional during vFiler creation)
- Script path (optional)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Click **Add** to start the **Add vFiler Unit** wizard.
3. Enter or select information as requested in the wizard, then click **Finish**.

You can complete the entire vFiler configuration or you can create an inactive vFiler unit and complete the protocol or network setup later.

You can verify that the vFiler unit you added is included in the hosts list in the **vFiler Units** window.

If you provided all of the required information during the create process, you can now protect or provision data that is associated with the new vFiler unit.

If you did not specify all of the vFiler unit information during the creation process, you can configure it later by using the **Setup vFiler Unit** wizard on the **Hosts > vFiler Units** window.

#### **Related concepts**

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

#### **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Decisions to make before setting up vFiler unit properties

---

Before starting the **Setup vFiler Unit** wizard to configure vFiler storage unit properties, it is useful to have all of the configuration information available for the unit that are you configuring.

Use the vFiler Setup option to add or modify vFiler unit attributes. For example, if you assigned but did not configure the CIFS protocol when you created the vFiler unit, you can use the **Setup vFiler Unit** wizard to perform the CIFS configuration.

<b>Allowed protocols</b>	What assigned protocols do you want to add or change on the vFiler unit?  The following protocols are supported: <ul style="list-style-type: none"><li>• NFS</li><li>• CIFS</li><li>• iSCSI</li></ul>
	Fibre Channel is <i>not</i> supported on vFiler units.
	<b>Attention:</b> If you assign the CIFS protocol to the vFiler unit, you need to set up CIFS before you can use the vFiler unit. Performing the setup stops and restarts CIFS, interrupting the CIFS service.
<b>IP address</b>	What IP address do you want for the vFiler unit?  The IP address accepts both IPv4 and IPv6 address formats.
<b>Network mask</b>	What network mask do you want for the vFiler unit?  <b>Note:</b> The Network mask accepts both IPv4 and IPv6 address formats. When using IPV4 format, use four octet notation. When using IPV6 format, specify the network mask length (the number of bits, from 1 to 127).
<b>Network interface</b>	What Ethernet interface do you want to add or change for the vFiler unit?  The Ethernet interface is not required to create the vFiler unit, although you must specify an interface before you can use the vFiler unit. If you plan to run scripts on the vFiler unit, you might choose to wait to specify the Ethernet interface later, by using the Setup option.
<b>VLAN ID</b>	Do you want to specify a VLAN ID?  VLANs allow you to partition a physical network into multiple virtual networks that are totally separate from one another.

If the vFiler unit that you plan to add is created on an active/active host, you can use an existing VLAN ID or create a new VLAN ID for the vFiler unit.

**Partner interface** What partner interface do you want?

If you are using an active/active host in the setup of the vFiler unit, the partner interface is selected automatically. If no partner interface is configured, then the column is not visible.

The storage system on which the vFiler unit is created must be configured as an active/active configuration before setting up the vFiler unit.

**vFiler template** Which vFiler template do you want?

You must reselect a vFiler template during setup. A vFiler template is a set of vFiler configuration settings and the corresponding CIFS configuration settings.

**Attention:** The **Setup vFiler Unit** wizard does not remember the vFiler template used during the vFiler unit creation. If you do not select the vFiler template you originally used, the network settings are cleared.

**CIFS workgroup name** What Windows workgroup name do you want for the CIFS setup?

The Windows workgroup name specifies the name of the shared resources. The workgroup name option is displayed if the following apply:

- You select the CIFS protocol
- You select the Perform CIFS setup option
- You do not select a vFiler template or the template you select does not include CIFS settings

If you set up the vFiler unit to use the CIFS protocol, the vFiler units can use the same computer names as the servers. This enables CIFS clients to share resources without having to remap their drives or search for the new server.

**CIFS domain user and domain password** What CIFS domain user ID and password do you want?

You can enter a login name and password for administrative access to the Active Directory system. The Domain User and Domain Password options are displayed if the following apply:

- You select the CIFS protocol
- You select the Perform CIFS setup option
- You select a vFiler template that specifies Active Directory for CIFS authentication

<b>Root password</b>	Which vFiler unit root password do you want?  If you did not choose a root password when you created the vFiler unit, you must choose one before you can use the vFiler unit.
<b>Script path</b>	Do you want to use a custom script to help manage vFiler units? If so, what is the full path of the script?  You can use the script while creating or setting up the vFiler unit.  <b>Note:</b> If the DataFabric Manager server is running on Windows, and if the post-setup script for the vFiler unit is on a network share, the script location must be specified by the full UNC path (no drive letter mapping).

### Related tasks

[\*Setting up vFiler unit properties\*](#) on page 935



# Considerations for active/active hosts

---

When using an active/active host in the creation or setup of a vFiler unit, the following are important considerations.

- If you want to use an active/active host in creating your vFiler unit, you need to configure the storage systems before creating the vFiler unit.
- In order to have appropriate failover behavior, you need to configure new IP space and VLAN interface when creating the vFiler unit.
- If you are creating a vFiler unit using non-default IP space, Provisioning Manager moves the partner interface to the non-default IP space of the primary vFiler unit.
- If you are creating a VLAN as part of the vFiler unit creation or setup, a corresponding VLAN will be setup on the partner interface.

## Related concepts

[\*Decisions to make before adding a vFiler unit\*](#) on page 923

## Related tasks

[\*Setting up vFiler unit properties\*](#) on page 935



# Setting up vFiler unit properties

---

After you create a vFiler unit, you can configure the CIFS protocol, if you assigned one, or edit vFiler unit attributes by using the **Setup vFiler Unit** wizard.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

Have the following information available for the vFiler unit that you want to configure:

- Allowed protocols
- IP address
- Network mask
- Network interface
- VLAN ID information (optional in an active/active configuration)
- Partner interface to use in an active/active configuration
- vFiler template name
- Root password
- CIFS Windows Workgroup Name or Active Directory Domain User and Domain Password
- Script path (optional)

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit from the list and click **Setup** to open the **Setup vFiler Unit** wizard.

You can view the current configuration information of the vFiler to ensure that you do not override any information you do not want to change.

3. Modify the vFiler attributes that you want to change.

If you assigned the CIFS protocol to the vFiler unit, select the **Perform CIFS setup** check box to complete the CIFS domain authentication, then enter the appropriate information.

4. Click **Finish**.

You can see your changes in the details section of the **vFiler Units** window.

## Related concepts

*Decisions to make before setting up vFiler unit properties* on page 929

*Considerations for active/active hosts* on page 933

**Related references**

*Administrator roles and capabilities* on page 1055

# Editing storage system properties

---

You can change the login or NDMP credentials of storage systems and you can add licenses to storage systems that are managed by NetApp Management Console . The storage system properties sheet is particularly useful for modifying the credentials for multiple systems at one time.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If you do not have the proper privileges, you cannot select the credentials or licenses in the storage system property sheet.

## Steps

1. From the navigation pane, click **Hosts > Storage Systems** .
2. Select a host name from the host list.

If you have hosts that use the same user name and password, you can select multiple hosts to configure the same credentials on all the selected hosts. License information can only be edited on one host at a time.

3. Click **Edit** to open the properties sheet for the selected host.

You can edit the login credentials and the NDMP credentials for the selected host or add licenses to the host.

4. Verify that the changes you made to the storage system have been implemented.

You can view the properties information provided in the **Storage Systems Hosts** window.

The host credentials are updated in the DataFabric Manager database. It might take several minutes for the updated status to be reflected in the Login Credentials field for each selected host.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Editing Open Systems SnapVault properties

---

You can change the NetApp Host Agent password or the NDMP credentials for the Open Systems SnapVault hosts that are managed by NetApp Management Console.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

If you are editing an Open Systems SnapVault host that resides on a VMware ESX 3.5 server, see the guidelines for editing an Open Systems SnapVault host on a VMware ESX 3.5 server.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. Select an Open Systems SnapVault host name from the host list.

If you have hosts that use the same user name and password, you can select multiple hosts to configure the same credentials on all the selected hosts.

3. Click **Edit** to open the properties sheet for the selected host.

**Note:** The default NetApp Host Agent user name is "admin", which cannot be changed.

4. Verify that the changes you made to the host have been implemented.

You can view the properties information provided under **Hosts > OSSV**.

The NDMP credentials for the selected host are updated in the DataFabric Manager database. It might take several minutes for the updated status to be reflected in the NDMP Credentials field for the selected host.

## Related references

[Guidelines for adding and editing an Open Systems SnapVault host on an ESX server](#) on page 919

[Administrator roles and capabilities](#) on page 1055



# Stopping Open Systems SnapVault agents

---

You can stop the Open Systems SnapVault agent to perform maintenance on one or more selected clients or to reconfigure Open Systems SnapVault. When troubleshooting protection errors on a client running Open Systems SnapVault, stopping and then restarting the Open Systems SnapVault agent might solve the problem.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

There is no Open Systems SnapVault plugin for Solaris. Therefore, management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console on Solaris systems.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients on which you want to stop Open Systems SnapVault services.
3. Click **Stop**.

**Note:** Stopping the Open Systems SnapVault agent on a client causes the backup service on that client to stop. Be sure to restart the agent if you want to resume backup protection.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Starting Open Systems SnapVault agents

---

When you are troubleshooting protection errors on a client running Open Systems SnapVault, stopping and then restarting the Open Systems SnapVault agent might solve the problem.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

There is no Open Systems SnapVault plugin for Solaris. Therefore, management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console on Solaris systems.

If you stop Open Systems SnapVault services to troubleshoot a problem or to perform maintenance, be sure to restart the Open Systems SnapVault agent when you are ready to resume services.

## Steps

1. From the navigation pane, click **Hosts ▶ OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients on which you want to start or resume Open Systems SnapVault services.
3. Click **Start**.

The Open Systems SnapVault agent starts on each selected client, and backup service starts or resumes on each client according to its schedule.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Updating Open Systems SnapVault client data

---

Data shown in the list of Open Systems SnapVault clients is gathered at regular intervals. If you are trying to troubleshoot a problem with an Open Systems SnapVault client, you can update the data for that client as needed to view the most current status.

## Before you begin

The client must be running the Open Systems SnapVault 2.3 or later agent and NetApp Host Agent 2.3.1 or later.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. From the list of Open Systems SnapVault clients, select one or more clients for which you want to update data.
3. Click **Refresh**.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Diagnosing a storage system

---

You can use the **Diagnose Storage Systems** wizard to verify the configuration for your storage system. You can also make necessary changes to some of the storage system properties and enable SnapMirror and SnapVault licenses from the diagnostics wizard.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

When running the diagnostics wizard, it can be useful to have the following information available to verify for the storage system that you want to diagnose:

- Host Name
- Domain Name
- IP Address
- Licenses that should be enabled for the storage system
- SnapMirror Access Control List for the storage system, if licensed for SnapMirror
- SnapVault Access Control List for the storage system, if licensed for SnapVault
- Login Credentials (user name and password)
- NDMP Credentials (user name and password)

**Note:** The credentials of a vFiler unit always have a status of Not Applicable. This status for a vFiler unit does not indicate a problem.

## Steps

1. From the navigation pane, click **Hosts ▶ Storage Systems**.
2. Click **Diagnose** to start the wizard, then verify or modify information as requested in the wizard.

The diagnostics wizard checks the configuration of hosts.
3. Verify that any changes that you made to your host configuration are displayed in the storage systems list in the **Storage Systems Hosts** window.

If configuration changes are made to a host from an interface other than NetApp Management Console , you might need to use the Refresh button to pull those changes into the host list for viewing in the console.

## Related concepts

[Ways to investigate problems with hosts](#) on page 903

**Related references**

*Administrator roles and capabilities* on page 1055

# Diagnosing an Open Systems SnapVault host

---

You can use the **Diagnose OSSV Host** wizard to verify your Open Systems SnapVault configuration and to make necessary changes to some Open Systems SnapVault properties.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

When running the diagnostics wizard, it can be useful to have the following information available to verify for the Open Systems SnapVault host that you want to diagnose:

- Host Name
- Domain Name
- IP Address
- NetApp Host Agent port number
- Operating system credentials for the host on which NetApp Host Agent is running, if you would like to use DataFabric Manager to update and manage the credentials for you
- NDMP Credentials (user name, password, and port number)

## About this task

When diagnosing issues on Solaris systems, note that there is no Open Systems SnapVault plugin for Solaris, so the NetApp Host Agent cannot talk to the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent cannot be performed from the management console.

## Steps

1. From the navigation pane, click **Hosts > OSSV**.
2. Click **Diagnose** to start the wizard. Verify or modify information as requested in the wizard.
3. Verify that any changes you made are displayed in the hosts list in the **OSSV Hosts** window.

You might need to refresh the window before you can view the changes in the hosts list.

## Related concepts

[Ways to investigate problems with hosts](#) on page 903

## Related references

[Administrator roles and capabilities](#) on page 1055



# vFiler unit migration overview

---

You can migrate a vFiler unit to another storage system. If your storage strategy is focused on vFiler units as containers for datasets; you can migrate a vFiler unit when one or more datasets are completely contained by that vFiler unit.

## Related concepts

[\*Description of migration tasks\*](#) on page 955



## vFiler unit migration requirements

---

A vFiler unit must meet the following requirements before you can migrate it to another vFiler unit.

- A vFiler unit that has its root storage as a qtree in a volume that is not owned by the vFiler unit can be migrated. However, the backup Snapshot copies of that qtree cannot be migrated.
- The vFiler unit cannot have volumes that are destinations of backup or mirror relationships.
- All qtrees contained by the vFiler unit must be in a volume that belongs to the vFiler unit. The exception is a qtree that contains root storage for the vFiler unit.
- The vFiler unit must be running Data ONTAP release 7.3.1 or later.



# Description of migration tasks

---

A complete migration of a dataset or vFiler unit includes all of the following operations. Each operation can be initiated separately on the **Datasets** window Migration tab or on the **vFiler Units** window.

## Next topics

- [\*Migration Step 1. Start\* on page 956](#)
- [\*Migration Step 2. Update \(optional\)\* on page 956](#)
- [\*Migration Step 3. Cutover\* on page 957](#)
- [\*Migration Step 4. Cleanup\* on page 958](#)
- [\*Manual cleanup after migration\* on page 958](#)

## Related concepts

- [\*vFiler unit migration overview\* on page 951](#)
- [\*Decisions to make before starting vFiler unit migration\* on page 959](#)
- [\*Dataset migration overview\* on page 769](#)
- [\*Dataset migration limitations\* on page 775](#)
- [\*Decisions to make before starting dataset migration\* on page 781](#)

## Related tasks

- [\*Starting a vFiler unit migration\* on page 961](#)
- [\*Updating vFiler unit migration SnapMirror relationships\* on page 963](#)
- [\*Cutting over to the new vFiler unit destination\* on page 965](#)
- [\*Cleaning up a vFiler unit migration\* on page 967](#)
- [\*Starting a dataset migration\* on page 783](#)
- [\*Updating dataset migration SnapMirror relationships\* on page 785](#)
- [\*Cutting over to the new dataset storage destination\* on page 787](#)
- [\*Cleaning up a dataset migration\* on page 789](#)

## Migration Step 1. Start

This operation begins data migration by starting the **Dataset Migration** wizard or the **vFiler Unit Migration** wizard, which starts a baseline transfer of the data to a new destination.

The licensed provisioning application performs the following tasks:

- Checks the destination storage system for the following:
  - The storage system has licenses for SnapMirror, MultiStore, and for all the allowed protocols of the source vFiler unit.
  - The vFiler unit limits for the storage system are not at a maximum level.
  - There are no name conflicts for all the source volumes.
  - There is space available for all the source volumes.
- Provisions destination storage according to the destination provisioning policy.  
For vFiler unit migrations in which the vFiler unit is a container of one or more datasets, the destination is provisioned according to the respective provisioning policies for each dataset.
- Creates the required IPspace and VLANs on the destination storage system.
- Starts the vFiler unit migration by starting the baseline transfer of the vFiler unit volumes.
- Polls for the SnapMirror transfers to complete.

If the provisioning application encounters a failure at any point in this operation, it undoes the entire process and reports the error.

## Migration Step 2. Update (optional)

This operation performs an on-demand update of the SnapMirror relationships that were created as part of the migration start operation. This operation is useful if a scheduled update fails, which causes the lag time of the SnapMirror relationships to increase to an undesirable length.

## Migration Step 3. Cutover

This operation stops access to the VFiler unit on the source storage system from which the data is served and enables access to the vFiler unit on the new destination storage system. You must shut down all applications using the dataset or vFiler unit before beginning the migration cutover operation.

Before performing the data source cutover to the new destination, the provisioning application verifies that the following is true:

- The IP addresses of the source vFiler unit are not in use in the same IPspace in the destination storage system.
- No error occurred in the last SnapMirror update on any of the SnapMirror relationships involved in migration.
- The destination storage system has the licenses for all allowed protocols on the vFiler unit.
- The aggregates hosting the destination volumes have enough space.
- All the volumes belonging to the source vFiler units or units have SnapMirror relationships to the destination volumes.

If any of these items is not true, the cutover of the data source to the new destination is not performed and an error is reported.

When all checks have passed, the provisioning application performs the following tasks:

- Runs the specified script
  - If a script is specified as part of the destination switch operation and it contains premigration operations, they are executed before the cutover is performed.
    - If a script is specified as part of the destination switch operation and it contains cutover operations, they are executed during the cutover operation. (This is useful when you have a script to quiesce an application.)
      - If the script contains postmigration operations, they are executed after the cutover is performed. (This is useful when you have a script to resume an application.)
  - Switches data access from the original source vFiler unit to the new destination VFiler unit and deletes the source vFiler unit.
    - The new destination vFiler unit becomes active, writable, and online.
- Suspends the datasets
  - This prevents new backups from starting during the migration.
- Removes volumes from the source dataset
  - As each volume is added to the new destination, the source volume is removed from the source dataset. Dynamic references in the source dataset are not removed; you must remove them manually after the migration cleanup operation finishes.
- Modifies the backup version tables to point to the new primary storage.
- Modifies all backup and mirror relationships to point to the new primary storage.

- Copies the history data in Operations Manager to reflect the new primary storage.
- Resumes the dataset operation.

When these tasks are finished, you can restart any applications that were shut down before the migration.

The provisioning application responds to failures as follows:

- If the data migration succeeds but the backup relationship migration fails, the dataset remains in suspended mode with the status Migrated-Errors.  
You must manually correct the errors. When the errors are corrected, you can use the Operations Manager CLI commands to change the migration status to Normal and then resume dataset operation.
- If the migration cutover operation fails, the source vFiler unit is brought back online, the status of the source dataset and vFiler unit is set to Migrate-Failed, and the destination storage is destroyed.

## Migration Step 4. Cleanup

This operation deletes the volumes that were used by the vFiler unit on the old data storage system. A preview window allows you to see which volumes will be destroyed. VLANs and IPspaces used by the old vFiler unit are not automatically destroyed; you must remove them manually after the migration cleanup operation finishes.

## Manual cleanup after migration

After all migration cleanup operation has finished successfully and the dataset or vFiler unit status has the status "Not started," you must use an application like FilerView to manually delete the following:

- Dynamic references in the old, source dataset.
- VLANs and IPspaces used by the old, source vFiler unit.

# Decisions to make before starting vFiler unit migration

---

Before you start a vFiler unit migration by using the **vFiler Unit Migration** wizard, it is useful to have ready all the migration information for the vFiler unit.

- |   |   |
|---|---|
| <b>Dataset migration commands or vFiler unit migration commands</b> | Are you migrating a dataset or a vFiler unit? <ul style="list-style-type: none"><li>• If there is a direct one-to-one correspondence between a dataset and a vFiler unit, you may use either the dataset migration commands or the vFiler unit migration commands.</li><li>• If a vFiler unit contains more than one dataset, and the storage for each dataset is completely owned by the vFiler unit, you should use the vFiler unit migration commands.</li><li>• If a vFiler unit contains more than one dataset, but the storage for at least one of the datasets is owned by more than one vFiler unit, you should use the dataset migration commands for each separate dataset.</li></ul> |
|---|---|

- |                                   |  |
|-----------------------------------|--|
| <b>Destination storage system</b> | What is the destination storage system for the migrated vFiler unit?<br>The wizard displays a list of the storage systems, from which you can select the destination storage system. |
|-----------------------------------|--|

**Note:** Because you can select storage systems that are not in the resource pool, the vFiler unit might not be in conformance after the migration. To avoid nonconformance, you can add the storage system to the resource pool before starting the migration.

- |                             |  |
|-----------------------------|--|
| <b>Interface selections</b> | What interfaces do you want to use?<br>You can select from a list of prepopulated IP addresses that displays the associated Netmask and Interface values and the prepopulated VLAN ID for each. Or you can modify the IP addresses and VLAN IDs, or you can add additional ones. |
|-----------------------------|--|

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Starting a vFiler unit migration](#) on page 961



# Starting a vFiler unit migration

---

You can begin migration of a vFiler unit by initiating the migration start operation, which starts the **vFiler Unit Migration** wizard and performs the first set of operations for the migration.

## Before you begin

Have available the information that you need to complete this task:

- Destination storage system (required)
- Interface to which the IP address will be bound to the destination storage system and the VLAN ID (required)
- Physical VLAN interface on which the VLAN will be created if VLANs are created during migration for the partner of the destination storage system (required if the destination storage system has an active/active configuration)

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You can cancel a vFiler unit migration anytime during the migration start operation.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Start migration** to start the **vFiler Unit Migration** wizard.
3. Complete the steps in the wizard to start the migration.

On the Interface Selection page of the wizard, you can specify a VLAN ID to create a tagged interface. However, you can tag only the base interfaces that are down.

To add more interfaces, click **Add**. To delete an interface, select it and click **Delete**.

You can check the job progress displayed in the Tracking Dataset Migration Job display popup window or you can move the popup window to the background and track the job progress in the **Jobs** window.

At any time after the migration start operation finishes successfully, you can update the SnapMirror relationships by initiating the migration update operation.

## After you finish

To continue the migration, you must manually initiate the migration cutover operation.

## **Related concepts**

[\*Decisions to make before starting vFiler unit migration\*](#) on page 959

[\*Description of migration tasks\*](#) on page 955

## **Related tasks**

[\*Updating vFiler unit migration SnapMirror relationships\*](#) on page 963

[\*Cutting over to the new vFiler unit destination\*](#) on page 965

[\*Canceling a vFiler unit migration\*](#) on page 969

## **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Updating vFiler unit migration SnapMirror relationships

---

After the migration start operation finishes, you can initiate an on-demand update of the SnapMirror relationships that were created as part of the migration start operation. This is an optional step in the vFiler migration process.

## Before you begin

You can perform this task only on a vFiler unit that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

This operation is useful if a scheduled update fails, which causes the lag time of the SnapMirror relationships to increase to an undesirable length. The migration

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Update** to update the SnapMirror relationships that were created as part of the migration start operation.
3. Click **Yes** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Jobs** window.

## After you finish

To continue the migration, you must manually initiate the migration cutover operation at a convenient time.

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Starting a vFiler unit migration](#) on page 961

[Cutting over to the new vFiler unit destination](#) on page 965

**Related references**

*Administrator roles and capabilities* on page 1055

# Cutting over to the new vFiler unit destination

---

After the migration start operation finishes, you can initiate the migration cutover operation to switch the old destination from which the data is served to the new destination and update the SnapMirror relationships.

## Before you begin

- You can perform this task only on a vFiler unit that has the status "Started, cutover required." This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.
- Because this is an automated offline migration, you must shut down all applications that use the vFiler unit.
- Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## About this task

You might want to initiate this operation at a time when the vFiler unit has a very low level of activity. When the migration cutover operation begins, you cannot cancel or reverse it.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Cutover**.
3. (Optional) In the confirmation dialog box, you can enter the name of a script to be executed.

For example, a script might quiesce an application and then resume the application.

4. Click **Cutover** in the confirmation dialog box to begin the operation.

After access to the data is switched over to the vFiler unit on the destination storage system, the backup versions, backup relationships, and DataFabric Manager history for the volumes are transferred to the destination storage system.

## After you finish

- To continue the migration, you must manually initiate the migration cleanup operation.
- You must restart all applications that use the data owned by the migrated vFiler unit.

## Related concepts

[Description of migration tasks](#) on page 955

## **Related tasks**

[\*Starting a vFiler unit migration\*](#) on page 961

[\*Updating vFiler unit migration SnapMirror relationships\*](#) on page 963

[\*Cleaning up a vFiler unit migration\*](#) on page 967

## **Related references**

[\*Administrator roles and capabilities\*](#) on page 1055

# Cleaning up a vFiler unit migration

---

After the migration cutover operation finishes, you can initiate the migration cleanup operation to delete the old storage.

## Before you begin

You can perform this task only on a vFiler unit that has the status "Migrated, cleanup required." This status indicates that the migration cutover operation is finished and access to the data is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. However, old storage needs to be deleted.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Select a vFiler unit and click **Cleanup**.

The Migration Cleanup confirmation dialog box lists the volumes on the old destination that will be deleted.

3. Click **Apply** in the confirmation dialog box to begin the operation.

## After you finish

To complete the migration process, you must manually perform the following cleanup tasks using an application like FilerView (if the VLANs and IPspaces are not shared):

- Delete dynamic references in the old source dataset.
- Delete VLANs and IPspaces used by the old source vFiler unit.

## Related concepts

[Description of migration tasks](#) on page 955

## Related tasks

[Cutting over to the new vFiler unit destination](#) on page 965

## Related references

[Administrator roles and capabilities](#) on page 1055



# Canceling a vFiler unit migration

---

You can cancel a vFiler unit migration at any time when the status is "started, cutover required." When you cancel a vFiler unit migration, the licensed provisioning application aborts all ongoing transfers and deletes all the provisioned storage on the destination storage system and on the destination vFiler unit.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Hosts > vFiler Units**.
2. Click **Cancel**.
3. In the confirmation dialog box, click **Yes**.

## After you finish

After you cancel a vFiler unit migration, you must manually delete the VLANs and IPspaces that were created on the destination storage system and vFiler unit.

## Related tasks

[Starting a vFiler unit migration](#) on page 961

## Related references

[Administrator roles and capabilities](#) on page 1055



# Viewing vFiler unit migration status

---

You can view the status of a vFiler migration operation in the **vFiler Units** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Step

1. From the navigation pane, click **Hosts > vFiler Units**.

The status is displayed in the "Migration status" column.

## Related references

[\*Administrator roles and capabilities\*](#) on page 1055



# Monitoring jobs

---

You can monitor for job status and other job details using the **Jobs** window.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data > Jobs**.

Only jobs for the selected resource group are displayed.

2. (Optional) Customize the **Jobs** window in any of the following ways:

- Select a resource group to see the jobs for that group.
- Select a job in the jobs list to see the details about that job.
- Use the View Jobs filter buttons to control the range of jobs you want displayed.
- Click  in a column header to control which job entries you want displayed.
- Click the sort arrows in a column header to change the sort order of the entries in that column.
- Click  in the upper-right corner of the list to select which columns are displayed.
- Drag the bottom of the jobs list area up or down to resize that area.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Canceling jobs

---

You might need to stop a job: for example, if a job is taking too long to complete, if a job is encountering too many errors, or if a job was started manually but is no longer needed.

## Before you begin

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Data ▶ Jobs**.  
Only jobs for the selected resource group are displayed.
2. From the list of jobs, select one or more jobs that are currently running.  
The status in the Progress column must be **Running**.
3. Click **Cancel**.
4. In the Cancel Jobs dialog box, click **Yes** to stop the selected job.

The Cancel Job Request Process Monitor window displays the progress of your cancel request and detailed information about any errors that occurred during the cancellation process.

## Related references

[Administrator roles and capabilities](#) on page 1055



# Where to view reports and logs

---

In general, you use your NetApp Management Console application to monitor jobs, events, and alarms associated with that application, and you use Operations Manager to monitor logs.

- To view reports of jobs, events, or alarms associated with most NetApp Management Console applications, use the NetApp Management Console System window.
- To view jobs, events, or alarms associated with your NetApp Management Console disaster recovery feature, use the Operations Manager Reports menu.

**Note:** After displaying the disaster recovery report, you can use the spreadsheet or print buttons to export the report to .XLS format or send it to the printer.

- To view DataFabric Manager or Operations Manager logs, use Operations Manager Reports menu.

**Note:** After displaying the report, you can use the spreadsheet or print buttons to export the report to .XLS format or send it to the printer.
- To view syslog cluster messages, use the tools available on the Operations Manager Cluster Console.

## Related tasks

[How do I back up data?](#) on page 589



# Dashboards > Provisioning

The **Provisioning Dashboards** window provides cumulative at-a-glance status information for space management issues related to datasets and resource pools. Further detail can be viewed on the Help page accessible from each dashboard panel.

You must be assigned the appropriate privileges to view the dashboard panels.

<b>Dataset Conformance Status</b>	Displays the total number of dataset members that are conforming to associated policies. Values can be Conformant or Nonconformant.
<b>Top Five Events</b>	Displays the five events with the highest severity levels, ordered by time. More detail about each event is provided in the <b>Events</b> window.
<b>Dataset Resource Status</b>	Displays the number of datasets at different levels of resource status severity. The status represents the worst event severity of all current events on all direct and indirect members of the dataset nodes. Values can be Emergency, Critical, Error, Warning, or Normal.
<b>Dataset Space Status</b>	Displays the total number of datasets being managed by NetApp Management Console , grouped according to their current space status value. The status represents the worst space status of all members in all nodes of the dataset. Events are generated at the dataset level when the space status of a dataset changes. Values can be Error, Warning, Normal, or Unknown.
<b>Resource Pool Space Status</b>	Displays the total number of resource pools that currently meet or exceed the space thresholds. Values can be Full, Nearly Full, Overcommitted, and Nearly Overcommitted.
<b>Resource Pools</b>	Displays, by resource pool name, the total space allocated to and the space utilization for each resource pool. Total Size values are indicated in numbers, such as gigabytes or terabytes. Utilization is indicated in percentage of the Total Size. Items are sorted by utilization percentage.

Click  on the title bar of each dashboard panel to replace the work area with another window related to the content of the panel.

Click  on a row of a dashboard panel to replace the work area with a window related to the content of the panel, with information highlighted that is relevant to that specific row in the panel.

You can filter the content of the dashboard panels, to focus on specific groups of datasets or resource pools, by using the Group selection list on the console tool bar.



# Dashboards > Provisioning > Dataset Conformance Status

---

You can use the **Dataset Conformance Status** panel to view how many datasets are either conformant or nonconformant with their policies.

## Status Descriptions

Conformance status indicates if all members of a dataset are conforming to all of the policies associated with the dataset.

<b>Conformant</b>	Status is normal. The dataset is configured in accordance with all associated policies.  A dataset is considered conformant if it is configured according to the dataset's protection policy and the provisioning policies attached to nodes of the dataset.
<b>Nonconformant</b>	Status is in error. The system is unable to bring the dataset into accordance with all associated policies.

Click  beside the dashboard panel title to replace the work area with the **Datasets** window.

You can filter the content of some of the dashboard panels by using the Group selection list on the management console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



# Dashboards > Provisioning > Dataset Resource Status

---

You can use **Dataset Resource Status** panel to view the overall status of all resources in a dataset.

## Status Descriptions

This dashboard panel displays the number of datasets that are at different levels of resource status severity. The status represents the worst event severity of all current events on all direct and indirect members of the dataset nodes.

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

Severity levels include the following.

<b>Emergency</b>	The event source unexpectedly stopped performing and experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
<b>Critical</b>	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
<b>Error</b>	The event source is still performing; however, corrective action is required to avoid service disruption.
<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds.
<b>Unknown</b>	Qtrees without quotas and non-qtree data will have resource status as Unknown.

Click  beside the dashboard panel title to replace the work area with the **Datasets** window.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



# Dashboards > Provisioning > Resource Pool Space Status

---

You can use the **Resource Pool Space Status** panel to view the number of resource pools that have exceeded or are about to exceed assigned space thresholds.

## Status Descriptions

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

- |                    |   |
|--------------------|---|
| <b>Full</b>        | Indicates the number of resource pools for which the used space has reached the Full threshold set for that resource pool. The amount of used space is determined based on the total used space for all aggregates in each resource pool.             |
| <b>Nearly Full</b> | Indicates the number of resource pools for which the used space has reached the Nearly Full threshold set for that resource pool. The amount of used space is determined based on the total used space for all aggregates in each resource pool.      |
| <b>Normal</b>      | Indicates the number of resource pools for which the total committed space in the resource pools is below the Resource Pool Nearly Full threshold. Total committed space is the sum of committed space of aggregates belonging to each resource pool. |

Click  beside the dashboard panel title to replace the work area with the **Resource Pools** window.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



## Dashboards ► Top Five Events

---

You can use the **Top Five Events** panel to view the five most severe events listed in the **Events** window and the source to which each event applies. The columns are ordered first by severity, then by time of the events.

Click  beside the dashboard panel title to replace the work area with the **Events** window. Descriptions of the events are provided in the online Help page for that window.

Click  on a row of the **Top Five Events** panel to replace the work area with the **Events** window, with information highlighted that is relevant to the selected row in the dashboard panel.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



## Dashboards > Resource Pools

---

You can use the **Dashboards > Resource Pools** to view the total space allocated to and the percentage of space utilized by each resource pool, listed by resource pool name.

Total Size values are indicated in numbers, such as gigabytes or terabytes. Utilization is given in percentages of the total allocated space per resource pool. Items are sorted in decreasing order of available space.

Click  beside the dashboard panel title to replace the work area with the **Resource Pools** window.

Click  on a row of a dashboard panel to replace the work area with the **Resource Pools** window, with information highlighted that is relevant to the selected row in the dashboard panel.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools. When you select a group filter, only relationships originating or terminating at an object in the selected group are listed.



# Dashboards > Provisioning > Dataset Space Status

You can use the **Dataset Space Status** panel to view how many datasets are at different levels of severity based on space available for the dataset.

## Status Descriptions

The dataset space status indicates if there are any dataset members with volumes that are running out of space, qtrees that are running out of quota, Snapshot copies that are exceeding the reserved space, and so forth. The status represents the worst space status of all members in all nodes of the dataset.

Events are generated at the dataset level when the space status of a dataset changes. Space status is calculated for a dataset only if a provisioning policy has been associated with the dataset node.

**Note:** If a status value is zero, the status item does not display in the dashboard panel.

<b>Error</b>	The event source is still performing, but corrective action is required to avoid service disruption.
<b>Warning</b>	The event source experienced an occurrence that you should be aware of. Events of this severity do not cause service disruption and corrective action might not be required.
<b>Normal</b>	A previous abnormal condition for the event source returned to a normal state and the event source is operating within the desired thresholds.
<b>Unknown</b>	The space status is not known. A number of conditions result in an Unknown state, including: <ul style="list-style-type: none"><li>• No provisioning policy attached to the dataset node</li><li>• Non-qtree data and qtrees without hard disk limits</li><li>• LUNs in a SAN environment, because there are no usage statistics for LUNs</li></ul>

Click  beside the dashboard panel title to replace the work area with the Provisioning tab on the **Datasets** window.

You can filter the content of some of the dashboard panels by using the Group selection list on the console tool bar. This option allows you to focus on information about a particular group, such as specific datasets or resource pools.



# Data ▶ Resource Pools

---

You can use the **Resource Pools** window to create, view, and modify collections of physical storage resources, called resource pools.

- [Command buttons](#) on page 993
- [Available resource pools list](#) on page 993
- [Resources tab](#) on page 994
- [Space breakout tab](#) on page 994
- [Dependencies tab](#) on page 994
- [Window customization](#) on page 995

When a resource pool is assigned to a dataset, data management applications use the resources in the resource pool to provision storage containers as needed by the dataset and according to the settings defined in policies assigned to the dataset.

## Command buttons

- |               |   |
|---------------|---|
| <b>Add</b>    | Starts a wizard that helps you create a new resource pool.  |
| <b>Edit</b>   | Opens the properties window for the selected resource pool. From the properties window you can modify the settings (Name, Description, Contact, Owner), assigned resources, labels, or space thresholds of an existing resource pool.   |
| <b>Delete</b> | Displays a dialog box that asks you to confirm that you want to delete the selected resource pool. You can either proceed with deleting the selected resource pool or cancel the activity. Deleting a resource pool currently assigned to a dataset also deletes any relationships created in accordance with a policy assigned to that dataset. Deleting a resource pool does <i>not</i> delete the physical resources that were in the resource pool. |

## Available resource pools list

This list displays key property settings and space management information for each of the resource pools.

- |                       |   |
|-----------------------|---|
| <b>Name</b>           | The name assigned to the resource pool.   |
| <b>Total Size</b>     | The total amount of storage space assigned to the resource pool.                            |
| <b>Available Size</b> | The amount of storage space available in the resource pool.                                 |
| <b>Utilization</b>    | The percentage of total storage space being used in the resource pool.                      |
| <b>Owner</b>          | The person who maintains or is responsible for the resource pool, such as an administrator. |

<b>Description</b>	A description that identifies the resource pool.
<b>Time Zone</b>	The time zone you want applied to the resource pool.
	<b>Note:</b> If a resource pool is assigned to a dataset using a Protection Manager policy, the time zone you select can impact the protection schedule. Make sure you understand the potential impact to any of your schedules before changing the Time Zone property.

## Resources tab

<b>Resources</b>	This area displays a tree view of the physical resources assigned to a selected resource pool. The physical resources associated with the selected resource pool are displayed in the expandable Resources list.
------------------	--

## Space breakout tab

The Space breakout tab lists the aggregates assigned to each selected resource pool. If you select one or more items in the list of available resource pools, the aggregates associated with each selected resource pool are displayed in the Space breakout list. If you added a storage system to a selected resource pool, each of its aggregates is listed separately.

<b>Aggregate</b>	The name of the aggregates in the selected resource pool.
<b>Total Size</b>	The total size of the listed aggregate.
<b>Committed Size</b>	The amount of space guaranteed to the volumes contained in the aggregate. This value can be higher than the total size of the aggregate. If you are using the aggregate overcommitment strategy, this value is expressed in KB, MB, GB, or TB.
<b>Available Size</b>	The amount of uncommitted space that is still available in the aggregate. This value is expressed in KB, MB, GB, or TB.
<b>Utilization</b>	The amount of currently used space out of the total size assigned to the aggregate, expressed in percentages.
<b>Datasets</b>	The names of datasets in the selected aggregate. If an aggregate is running out of space, you can use this list to choose which dataset to migrate.
<b>Used Space From Aggregate</b>	The amount of space on the aggregate that is used by the dataset.

## Dependencies tab

The Dependencies tab lists the datasets, if any, that use the selected resource pool and lists whether those datasets are capable of migration. This tab is displayed only when the provisioning license is installed.

<b>Dataset</b>	The datasets with which the selected resource pool is associated.
<b>Migration capable</b>	Whether a listed dataset is configured to be capable of migration.
<b>Remaining number of migration-enabled datasets allowed</b>	The number of additional datasets in the selected resource pool that can be configured for data migration.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Policies > Provisioning

---

You can use the **Provisioning Policies** window to view, add, edit, copy, or delete provisioning policies.

- [Command buttons](#) on page 997
- [Policies list](#) on page 997
- [Details tab](#) on page 998
- [Dependencies tab](#) on page 1000
- [Window customization](#) on page 1000

## Command buttons

<b>Add</b>	Starts the <b>Add Provisioning Policy</b> wizard, which allows you to configure and add a new provisioning policy.
<b>Edit</b>	Opens a window in which you can modify the properties of the selected provisioning policy.
<b>Copy</b>	Copies the selected provisioning policy and adds the copy as a new provisioning policy.
<b>Delete</b>	Opens a confirmation dialog box that you use to verify whether you want to delete the selected policies. You can delete a provisioning policy only if it has no dependencies: in other words, if the policy is not assigned to any datasets.

## Policies list

Displays the currently configured provisioning policies. The list is updated dynamically when the status changes. You can customize the display as follows:

<b>Name</b>	The name assigned to a provisioning policy.
<b>Storage Type</b>	The type of storage that the policy is configured to support:
<b>NAS</b>	The policy provisions NAS storage and exports storage for NAS access. NFS and CIFS protocols are supported.
<b>SAN</b>	The policy provisions SAN storage and exports storage for SAN access. FC and iSCSI protocols are supported.
<b>Secondary</b>	The policy provisions storage for secondary (backup or mirror) node. This type is available only if you have the Protection license also installed.

<b>Description</b>	An optional description of the provisioning policy. It might include the intended use of the provisioning policy or some other common attribute that identifies why the provisioning policy was created.
<b>Resource Label</b>	An optional text string that is used in provisioning requests as a filter for specific resources. Only storage resources that match the label are used for provisioning.  To display this column, you click  in the upper-right corner of the policies list.

## Details tab

Displays detailed configuration information about the selected policy. Only the properties applicable to the selected policy are displayed.

<b>Name</b>	The name assigned to the selected provisioning policy.
<b>Space utilization properties (for NAS storage only)</b>	<b>Guarantee space for dataset</b> If this option is enabled, the requested space is guaranteed for data and for Snapshot copies and guaranteed from the resource pool or pools associated with the dataset. Therefore, writes to a specified FlexVol volume or writes to files with space reservations enabled cannot fail because of a lack of available space in the containing aggregate.  If this option is disabled, the space is allocated on demand as data or Snapshot copies are written to datasets; some write requests might fail.  <b>Reserve space for Snapshot copies</b> If this option is enabled, an additional 20 percent of the requested space is provisioned from the resource pool or pools for Snapshot copies for every provisioned member in the dataset. This guarantees that Snapshot copies cannot fail because of a lack of disk space.  If this option is disabled, no additional Snapshot copy space is provisioned and Snapshot copies might fail if there is not enough space available.  <b>Guarantee maximum size</b> If this option is enabled, the maximum size of the requested space is guaranteed from the resource pool or pools associated with the dataset.  <b>Increase container size automatically</b> If this option is enabled, the initial space is guaranteed from the resource pool or pools associated with the dataset; the maximum space is allocated when needed. Snapshot copies are automatically deleted when additional space is needed. This option is available only for storage systems that are running Data ONTAP 7.3.1 or later.

<b>Quota settings (for NAS storage only)</b>	The default size of user quotas and group quotas. Quotas limit resource usage and provide notification when resource usage reaches specified levels.	
<b>SAN container properties (for SAN storage only)</b>	The SAN container type to be used for provisioning, as well as additional provisioning details:	
<b>Type of container to provision</b>	The SAN container type to be used for provisioning: Volume or LUN.	
<b>Space for data</b>	<b>Guaranteed</b>	Space for data is guaranteed on the SAN container.
	<b>On demand</b>	Space for data is not guaranteed on the SAN container. Space might need to be allocated manually.
<b>Space for Snapshot copies</b>	<b>Guaranteed</b>	Space for Snapshot copies is guaranteed on the SAN container.
	<b>On demand</b>	Space for data is not guaranteed on the SAN container; the container is automatically increased when additional space for Snapshot copies is needed.
<b>Delete oldest Snapshot copies automatically</b>	<p>If this option is enabled and a storage container needs more space, the Data ONTAP autosize option is used to automatically delete Snapshot copies to make more space available. To use this option, your storage must be using Data ONTAP 7.2.4 or later.</p> <p>If this option is disabled, Snapshot copies are not automatically deleted when a storage container needs more space; therefore, you might need to delete them manually.</p>	
<b>Space utilization thresholds</b>	Whether the licensed application generates space utilization events when a threshold is reached and, if so, the threshold settings for the Full and Nearly Full thresholds. The licensed application uses the thresholds to compute dataset space status and generate events.	
<b>Generate space utilization events</b>	<p>If this option is enabled, event notifications are generated when a space threshold is reached.</p> <p>If this option is disabled, no event notifications are generated when a space threshold is reached.</p>	

<b>Nearly Full threshold</b>	The percentage of the maximum size of a dataset at which a Nearly Full threshold event notification is generated.
<b>Full threshold</b>	The percentage of the maximum size of a dataset at which a Full threshold event notification is generated.
<b>Provisioning Script</b>	The full DataFabric Manager server path of a provisioning script that performs custom tasks after storage is provisioned.
<b>Deduplication properties</b>	<b>Deduplication status</b> Whether or not deduplication is enabled on the dataset node that is assigned the selected provisioning policy. <b>Deduplication schedule</b> The mode of deduplication, if any, that is enabled for the selected policy.  <b>Manual</b> Indicates that on-demand deduplication mode (in which deduplication not scheduled but is carried out only when you click "Dedupe Now") is enabled on the dataset node that is assigned the selected provisioning policy. <b>Auto</b> Indicates that automated deduplication mode (in which deduplication is started automatically based on the amount of new data in the volume) is enabled on the dataset node that is assigned the selected provisioning policy. <b>Custom</b> Indicates that scheduled deduplication mode (in which deduplication is implemented on a customized schedule) is enabled on the dataset node that is assigned the selected provisioning policy.

## Dependencies tab

Displays all of the datasets that are provisioned using the selected policy.

<b>Dataset Name</b>	The name of a dataset or dataset member to which the selected provisioning policy is assigned.
<b>Dataset Node</b>	The type of storage node: primary storage node or secondary storage node.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.

Click the column header to display the sort arrow.

- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Policies ► vFiler Templates

---

You can use the **vFiler Templates** window to view, add, edit, copy, or delete vFiler templates.

- [Command buttons](#) on page 1003
- [vFiler Templates list](#) on page 1003
- [Details area: General](#) on page 1003
- [Details area: CIFS Settings](#) on page 1004
- [Window customization](#) on page 1004

## Command buttons

<b>Add</b>	Starts the <b>Add vFiler Template</b> wizard which allows you to configure and add a new vFiler template.
<b>Edit</b>	Opens a property sheet in which you can modify the properties of the selected vFiler template.
<b>Copy</b>	Copies the selected vFiler template and adds the copy as a new vFiler template.
<b>Delete</b>	Deletes the selected vFiler templates.

## vFiler Templates list

<b>Name</b>	The name of the vFiler template.
<b>Description</b>	The description provided when the vFiler template was configured.
<b>CIFS Authentication Mode</b>	The name of the CIFS domain to which a vFiler unit using the selected vFiler template belongs. Valid values are: <ul style="list-style-type: none"> <li>• Active directory</li> <li>• Windows workgroup</li> </ul>
<b>DNS Domain</b>	The name of the domain or the IP address of the PDC.

## Details area: General

Displays additional general configuration information about the selected vFiler template. Options marked with a checkmark (✓) are configured; options marked with an X are not configured.

<b>Name</b>	The name of the selected vFiler template.
<b>Description</b>	The description provided when the vFiler template was configured.

<b>Administrative Host</b>	The host name or the IP address of the host that has root access to the files needed to manage a vFiler unit using the selected vFiler template.
<b>DNS Domain</b>	The name of the DNS domain to which a vFiler unit using the selected vFiler template belongs.
<b>NIS Domain</b>	The name of the NIS domain to which a vFiler unit using the selected vFiler template belongs.

### Details area: CIFS Settings

Displays detailed CIFS configuration information about the selected vFiler template.

<b>Authentication Mode</b>	The mode used to authenticate data requests to or from a vFiler unit using this vFiler template. Valid values are:
	<ul style="list-style-type: none"><li>• Active directory</li><li>• Windows workgroup</li></ul>
<b>Security Protocol</b>	The security protocol to be used by a vFiler unit using this vFiler template. Valid values are:
	<ul style="list-style-type: none"><li>• NTFS-only</li><li>• Multiprotocol</li></ul>
<b>CIFS Domain</b>	The name of the CIFS domain to which a vFiler unit using the selected vFiler template belongs.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Hosts > Storage Systems

---

You can use the **Storage Systems Hosts** window to view detailed information about storage systems discovered by DataFabric Manager. From this window, you can add a storage system to NetApp Management Console, edit the properties on existing storage, and diagnose a storage system's configuration. You can also manage Data ONTAP service licenses.

- [Command buttons](#) on page 1005
- [Storage system host list](#) on page 1005
- [Details tab](#) on page 1006
- [Usage tab](#) on page 1010
- [Paths tab](#) on page 1010
- [Input Relationships tab](#) on page 1010
- [Output Relationships tab](#) on page 1011
- [Window customization](#) on page 1011

## Command buttons

<b>Add</b>	Starts the <b>Add Storage System</b> wizard, which allows you to set up storage system hosts.
<b>Edit</b>	Opens a window in which you can modify the properties of the selected host.
<b>Diagnose</b>	Starts the <b>Diagnose Storage Systems</b> wizard, which allows you to modify some aspects of a storage system's configuration.
	This button is disabled if more than one host is selected in the hosts list.
<b>Refresh</b>	Updates the host list for the selected host.

## Storage system host list

<b>Name</b>	Displays the name of the storage system or vFiler unit as it appears in the DataFabric Manager database.
<b>System Status</b>	Displays the current status of the storage system. Possible values are Online, Offline, and Unknown.  The default monitoring interval is one minute. The interval is specified as the Ping Monitoring Interval in Operations Manager.
	You can use the Options page in Operations Manager to view or change the interval. See the Operations Manager online Help for details.

<b>Login Credentials</b>	Displays the current status of the login credentials that DataFabric Manager uses to log in to the host.  Possible values are Good, Bad, Read Only, Unknown, and Not Applicable. NDMP credentials for vFiler units are designated Not Applicable because DataFabric Manager uses the credentials of the hosting system.
<b>NDMP Status</b>	The Network Data Management Protocol (NDMP) availability of the storage system as of the most recent NDMP monitoring check.  Possible values are Up, Down, and Unknown. The default interval for NDMP monitoring is 30 minutes. You can use the Backup Discovery Options page in Operations Manager to change the NDMP monitoring interval. See the Operations Manager online Help for instructions.
<b>NDMP Credentials</b>	Displays the current status of the Network Data Management Protocol credentials that DataFabric Manager uses to communicate with the host.  Possible values are Good, Bad, Unknown, and Not Applicable. NDMP credentials for vFiler units are always designated Not Applicable because DataFabric Manager uses the credentials of the hosting system. You can use the NDMP Credentials page in Operations Manager to edit the credentials for NDMP discovery. See the Operations Manager online Help for details.

## Details tab

The Details tab has four areas: General, Credentials, Service status, and Licenses.

<b>General</b>	
<b>IP Address</b>	Specifies the IP address associated with the selected storage system.
<b>Model</b>	Displays the model number of this storage system.
<b>Mirrored</b>	Indicates whether the SnapMirror license is enabled on this host. Possible values are Yes and No.
<b>Backup Destination</b>	Indicates whether a SnapVault Secondary license is enabled on this host, making the host a potential destination for backups.  Possible values are Yes and No.
<b>Backup Source</b>	Indicates whether the SnapVaultData ONTAP Primary license is enabled on this host, making the host a potential source of backups.  Possible values are Yes and No.  <b>Note:</b> Other hosts might also be potential backup sources, but the SnapVault Primary licenses for Linux, UNIX, and Windows are installed on the secondary system. This list confirms only

whether the SnapVaultData ONTAP Primary license is enabled on the host.

#### Credentials

	<b>Login User Name</b>	The name that DataFabric Manager uses to log in to the selected host.
	<b>NDMP User Name</b>	The name that DataFabric Manager uses to log in to the selected host by using NDMP.

#### Service status

<b>NFS</b>	Indicates whether the Network File System (NFS) service is Up or Down.
<b>CIFS</b>	Indicates whether the Common Internet File System (CIFS) service is Up or Down.
<b>iSCSI</b>	Indicates whether the iSCSI service is Up or Down.
<b>FC</b>	Indicates whether the Fibre Channel (FC) protocol service is Up or Down.

#### Licenses

The following licenses each enable a service of Data ONTAP.

You must enter a software license code on the storage system to enable the corresponding service. You do not need to indicate which license the code enables. The code is matched automatically to the appropriate service license.

<b>SnapMirror</b>	You install the SnapMirror licenses on both the source and destination storage systems for the mirror-copied data.  If the source and destination volumes are on the same system, only one license is required. SnapMirror replicates data to one or more networked storage systems. SnapMirror updates the mirror-copied data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on nonproduction systems, online data migration, and so on. You can also enable the SnapMirror license to use Qtree SnapMirror for backup.
-------------------	--

#### SnapVault Data ONTAP Secondary

You install the SnapVault Secondary license on storage systems hosting the backups of protected data.  
  
SnapVault creates backups of data stored on multiple primary storage systems and copies the backups to a secondary storage system. If data loss or corruption occurs, backed-up data can be restored to a primary or open storage system with little of the downtime and uncertainty associated with conventional tape backup and restore operations.

<b>SnapVault Data ONTAP Primary</b>	You install the SnapVault Data ONTAP Primary license on storage systems running Data ONTAP that contain host data to be backed up.
<b>SnapVault Windows Primary</b>	You install the SnapVault Windows Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a Windows-based primary storage system running the Open Systems SnapVault agent.  A Windows-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>SnapVault Windows Open File Manager</b>	You install the SnapVault Open File Manager license on a <i>secondary</i> storage system to enable the backup of open files on Windows primary storage systems running the Open Systems SnapVault agent.  You must install the SnapVault Windows Primary license and the SnapVault Data ONTAP Secondary license on the secondary storage system before installing the SnapVault Open File Manager license.
<b>SnapVault UNIX Primary</b>	You install the SnapVault UNIX Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a UNIX-based primary storage system (AIX, HP-UX, or Solaris) running the Open Systems SnapVault agent.  A UNIX-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>SnapVault Linux Primary</b>	You install the SnapVault Linux Primary license on a <i>secondary</i> storage system, in addition to the SnapVault Secondary license, to support a Linux-based primary storage system running the Open Systems SnapVault agent.  A Linux-based primary storage system running the Open Systems SnapVault agent does not require a SnapVault license.
<b>NearStore Option</b>	The NearStore license enables your storage system to use transfer resources as conservatively as if it were optimized as a backup system.  This approach is useful when the storage system on which you want to store backed-up data is not a system optimized for storing backups, and you want to minimize the number of transfer resources the storage system requires. Storage systems using the NearStore license must meet the following criteria: <ul style="list-style-type: none"><li>• The storage system must be a FAS30xx , FAS31xx series , or FAS60xx system.</li><li>• The version of Data ONTAP software must be 7.1 or later.</li></ul>

	<ul style="list-style-type: none"><li>• If you plan to use the SnapVault service, the storage system must have a SnapVault secondary license enabled.</li></ul>
<b>Deduplication</b>	The deduplication license enables you to consolidate blocks of duplicate data into single blocks so that you can store more information using less storage space.  The storage system must have the Deduplication license enabled. If you want to run deduplication on FAS platforms, the NearStore personality license must also be enabled. Monitoring of the volume-level deduplication option is done as part of the core license.
<b>SnapMirror Sync</b>	The SnapMirror Sync license enables you to replicate data to the destination as soon as it is written to the source volume.  SnapMirror Sync is a feature of SnapMirror.
<b>FCP</b>	Fibre Channel (FC) protocol is a licensed service on the storage system that enables you to export LUNs and transfer block data to hosts using the SCSI protocol over a Fibre Channel fabric.
<b>CIFS</b>	Common Internet File System (CIFS) protocol is a licensed service for remote file access that runs over TCP/IP on the Windows operating system.  CIFS enables application access and file sharing across the Internet.
<b>NFS</b>	Network File System (NFS) is client/server application that runs over TCP/IP on the UNIX operating system.  NFS enables application access and file sharing across the Internet.
<b>iSCSI</b>	The iSCSI protocol is a licensed service on the storage system that enables you to transfer block data to hosts using the SCSI protocol over TCP/IP.  iSCSI supports Gigabit Ethernet and is often used in a SAN environment.
<b>MultiStore</b>	The MultiStore license enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems, called vFiler units, on the network.  Be sure that the host on which you intend to install the MultiStore license is running Data ONTAP 6.5 or later.

## Usage tab

The Usage tab provides information about the aggregates, volumes, and qtrees that are associated with any host selected from the host list.

**Resource Type** Displays a tree of the storage system and the aggregates, volumes, and qtrees on that system.

You can also select either aggregates, volumes, or qtrees to narrow the list of resources associated with the storage system that you selected.

**Dependencies** Displays the name of the resource pool or datasets associated with the storage system, aggregate, or volume selected in the Resource Type menu.

## Paths tab

The Paths tab provides information about data that is moving into and out of host paths on the selected storage system. You can use this information to identify dependencies on a selected storage system, aggregate, volume, or qtree.

**Data coming into host path** Displays an expandable list of locations from which data is being backed up or mirror-copied to the selected host path.

**Host path** Displays the host path for which incoming and outgoing data is shown.

You can view the flow of data into and out of the storage system as a whole or expand the list to select a specific aggregate, volume, or qtree and view the flow of data through the selected path. Using the Resource Type menu, you can also select aggregates, volumes, or qtrees to narrow down the listing of resources associated with the storage system you selected.

**Data coming out of host path** Displays an expandable list of locations to which data is being backed up or mirror-copied from the selected host path.

## Input Relationships tab

This tab displays information about systems that send backup or mirror-copy data to the selected system.

You can use this information to identify dependencies on a selected storage system before shutting the system down for maintenance or to assess the impact of an outage.

**Lag Status** Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.

**Lag** Displays the time elapsed since the last successful backup or mirror-copy update.

**Source** Displays the location of the backup or mirror-copy data that is being sent to the selected system.

<b>Type</b>	Displays the type of relationship that the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	Displays the name of the dataset to which the incoming data belongs.
<b>Destination</b>	Displays where the incoming data is being stored on the selected storage system.

### Output Relationships tab

This tab displays information about systems that receive backup or mirror-copy data from the selected system.

You can use this information to identify dependencies on a selected storage system before shutting the system down for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	Displays the time elapsed since the last successful backup or mirror-copy update.
<b>Source</b>	Displays the location of data on the system that is being backed up or mirror-copied to a secondary system.
<b>Type</b>	Displays the type of relationship the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	Displays the name of the dataset to which the outgoing data belongs.
<b>Destination</b>	Displays where the outgoing data is being stored on the destination system.

### Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data > Datasets > Provisioning

---

If you have the Provisioning license, you can use the Provisioning tab on the **Datasets** window to add provisioning policy-compliant volumes, LUNs, or qtrees to a dataset node. You can also survey available data and Snapshot copy space allocation on individual volumes, LUNs, or qtrees, and resize the volumes and qtrees or delete Snapshot copies on the volumes.

- [Command buttons](#) on page 1013
- [Datasets list](#) on page 1014
- [Current space breakout tab](#) on page 1014
- [Space usage history tab](#) on page 1017
- [Deduplication tab](#) on page 1019
- [Exports tab](#) on page 1020
- [Window customization](#) on page 1021

## Command buttons

<b>Provision</b>	Starts the <b>Provisioning</b> wizard to add new provisioning policy-compliant volumes, LUNs, or qtrees to a primary node of the dataset. The dataset node must have an assigned resource pool.
<b>Resize Storage (volumes or qtrees only)</b>	Opens the <b>Resize Storage</b> window, which allows you to increase or decrease the space allocated to the selected volume or qtree dataset member.
<b>Delete Storage (volumes, qtrees, and LUNs)</b>	<p>Deletes the selected volume, qtree, or LUN from the dataset. You can select and delete one or more volumes, qtrees, or LUNs at a time by holding down Shift or Ctrl and selecting the data members you want to delete.</p> <ul style="list-style-type: none"> <li>• When you delete a volume, the licensed application returns the space used by that volume to its containing aggregate.</li> <li>• When you delete a LUN, the licensed application returns the space used by that LUN to its containing volume or containing qtree.</li> <li>• When you delete a qtree, the licensed application returns the space used by that qtree to its containing volume.</li> </ul>
<b>Delete Snapshot copies (volumes only)</b>	Opens the Delete Snapshot Copies window, which allows you to make more space available for data storage on the selected volume by deleting the selected Snapshot copies.
<b>Dedupe Now</b>	If deduplication is enabled on a selected volume's dataset node, opens the dialog to run unscheduled On-demand deduplication on that volume.

<b>Abort Dedupe</b>	If deduplication is currently in progress on a selected volume, stops that deduplication operation. This button appears only if deduplication is in progress.
---------------------	---

## Datasets list

Displays the information about datasets and the volumes, qtrees, or LUNs in each dataset.

<b>Dataset list</b>	Displays a list of all the datasets in your group.
---------------------	--

<b>Dataset</b>	The name of the dataset.
<b>Failed Over (if the Disaster Recovery license is installed)</b>	The failover status of the dataset (Ready, Failing over, or Failed over).
<b>Space Status</b>	The status of the available space for the dataset (Normal, Warning, Error, Unknown).  If any member of a dataset has space allocation error or warning conditions, that dataset's space status indicates that condition. You can select a dataset to see which of its volumes, LUNs or qtrees is the cause of a space warning or error condition.

<b>Dataset members list</b>	Displays the volume, LUN, and qtree members of the selected dataset.
<b>Storage</b>	The name and path location of the volume, LUN, or qtree dataset member.
<b>Node Name</b>	The name of the dataset node on which a volume is located.
<b>Space Status</b>	The status of the available space for the dataset member (Normal , Warning, Error, Unknown).
<b>Total Space</b>	The total storage space allotted to the selected dataset member.
<b>Available Space</b>	The amount of allocated storage space still available on the dataset member.

## Current space breakout tab

This tab displays information about the current space allocation for the selected volume, LUN, or qtree dataset member. The graph on the lefthand side illustrates the information provided on the righthand side.

<b>Data (displayed for NAS storage)</b>	This section displays information about the data space allocation and usage for the selected data member.
<b>Used space</b>	The space that is currently used on the selected dataset member.
<b>Free space</b>	The unused space that is available for data on the selected dataset member.
<b>Total data space</b>	The total data space capacity on the selected dataset member.
<b>Data (displayed for SAN storage)</b>	This section displays information about the data space allocation and usage for the selected data member.
<b>Used space</b>	The space that is currently used on the selected dataset member. In SAN storage, Used space normally represents the LUNs in the volume.
<b>Data in overwrite reserve</b>	The amount of data, if any, that is spilled into the SAN storage overwrite reserve space.
<b>Total data space</b>	The total data space capacity on the selected dataset member.
<b>Snapshot (displayed for NAS storage)</b>	This section displays information about the space allocation for Snapshot copies and the usage for the selected data member.
<b>Used Snapshot space</b>	The space that is currently used for Snapshot copies on the selected volume (does not apply to qtrees).
<b>Free Snapshot space</b>	The space that is available for Snapshot copies on the selected volume (does not apply to qtrees).
<b>Snapshot reserve</b>	The total space capacity for Snapshot copies on the selected volume (does not apply to qtrees).
<b>Snapshot overflow</b>	The space used for Snapshot copies on the volume beyond the space reserved for them (does not apply to qtrees).
<b>Overwrite Reserve (displayed for SAN storage)</b>	This section displays information on the overwrite reserve set aside in SAN volumes for LUN or Snapshot spillover.
<b>Data in overwrite reserve</b>	The amount of data, if any, that is spilled into the SAN storage overwrite reserve space.
<b>Overwrite reserve available</b>	The amount of overwrite reserve space that remains available.

<b>Volume (displayed for NAS volumes)</b>	This section displays information about the total space allocation for the selected volume.
<b>Total volume size</b>	The total combined space for data and Snapshot copies allocated to the selected volume.
<b>Snapshot reserve</b>	The total Snapshot copy space capacity on the selected volume.
<b>Nearly Full threshold</b>	The maximum amount of data space that can be used before the application generates a Nearly Full event warning message.
<b>Full threshold</b>	The maximum amount of data space that can be used before the application generates a Full event error message.
<b>Space Guarantee</b>	The type of space guarantee configured for the selected flexible volume (None, File, or Volume).
<b>Space Status</b>	The status of the available space for the selected volume (Normal, Warning, Error, Unknown). For explanations for Warning or Error status, click  to the right.
<b>Volume (displayed for SAN storage)</b>	This section displays information about the total space allocation for the selected SAN volume.
<b>Total volume size</b>	The total combined space for data and Snapshot copies allocated to the selected volume.
<b>Nearly Full threshold</b>	The maximum amount of data space that can be used before the application generates a Nearly Full event warning message.
<b>Full threshold</b>	The maximum amount of data space that can be used before the application generates a Full event error message.
<b>Used Snapshot space</b>	The amount of used Snapshot space on the selected SAN volume.
<b>Data and overwrite reserve size</b>	The total combined space set aside for data and the overwrite reserve.
<b>Volume used</b>	The total amount of SAN volume space used.
<b>Volume available</b>	The total volume space available.
<b>Space Guarantee</b>	The type of space guarantee configured for the selected SAN volume (None, File, or Volume).

<b>Space Status</b>	The status of the available space for the selected SAN volume (Normal , Warning, Error, Unknown). For explanations for Warning or Error status, click  to the right.
<b>Qtree space</b>	This section displays information about the total space allocation for the selected qtree.
<b>Qtree used space</b>	The space on the selected qtree currently used for data.
<b>Qtree free space</b>	The space allocated to the selected qtree that is currently not used.
<b>Qtree quota</b>	The space currently allocated to the selected qtree.
<b>Space Status</b>	The status of the available space for the selected qtree (Normal , Warning, Error, Unknown). For explanations for Warning or Error status, click  to the right.

### Space usage history tab

This tab graphically displays the history of space allocation and use on the selected volume or qtree over the selected period of time. This applies only to qtrees that have quotas settings configured.

To display space allocation data for a specific date and time, place your cursor at that date and time along the graph's time axis. The information for the cursor-selected date and time is displayed to the right of the graph.

<b>Time-period tabs</b>	Displays the space usage history on the selected volume or qtree during the selected time period (1 day, 1 week, 1 month, 3 months, 1 year).
<b>Data (displayed for NAS storage)</b>	Displays the space usage history for data on the selected volume or qtree during the selected time period.
<b>Total volume size</b>	The total combined space for data and Snapshot copies allocated to the selected volume at or during the selected time period.
<b>Used space</b>	The space used for data storage on the selected volume or qtree at or during the selected time period.
<b>Free space</b>	The unused space that is available for data on the selected volume or qtree at or during the selected time period.
<b>Total data space</b>	The total data space capacity on the selected volume or qtree at or during the selected time period.

<b>Volume (displayed for SAN storage)</b>	Displays the space usage history for data on the selected volume or qtree during the selected time period.
<b>Data and overwrite reserve size</b>	The combined space used by data and the overwrite reserve at or during the selected time period.
<b>Used Snapshot space</b>	Space on the selected volume used for Snapshot copies at or during the selected time period
<b>Volume used</b>	The amount of the selected volume that was used at or during the selected time period.
<b>Volume available</b>	The amount of space on the selected volume that was available at or during the selected time period.
<b>Total volume size</b>	The total combined space for data and Snapshot copies allocated to the selected volume at or during the selected time period.
<b>Snapshot (displayed for NAS volumes)</b>	Displays the space usage history for Snapshot copies on the selected volume during the selected time period.
<b>Used Snapshot space</b>	The space used for Snapshot copies on the selected volume at or during the selected time period.
<b>Free Snapshot space</b>	The unused space that is available for Snapshot copies on the selected volume at or during the selected time period.
<b>Snapshot reserve</b>	The total space capacity for Snapshot copies on the selected volume at or during the selected time period.
<b>Snapshot overflow</b>	The space used for Snapshot copies on the volume at or during the selected time period beyond the space reserved for them.
<b>Qtree space (Qtrees with quotas only)</b>	Displays the space usage history for the selected Qtree during the selected time period.
<b>Qtree used space</b>	The amount of Qtree space that was used during the selected time period.
<b>Qtree free space</b>	The amount of Qtree space that was available during the selected period.
<b>Qtree quota</b>	The amount of space that was allotted by quota to the Qtree during the selected period.

## Deduplication tab

This tab graphically displays the deduplication-related space savings on a selected volume if deduplication has been enabled and run for that volume. The information on deduplication savings is displayed to the right of the graph.

**Note:** If deduplication is enabled but has never been run on the selected volume, the Deduplication tab displays "Dedupe has not been run on the volume."

**With dedupe (Current state)** Graphs the current space usage with deduplication applied on the selected volume.

**Without dedupe** Graphs what space usage would be without deduplication applied on the selected volume.

**Volume** Displays a legend for the space usage components that are displayed in the "Without deduplication" and "With deduplication" graphs and also displays numerical values for those components.

### Used space

- In the "With dedupe" column: The amount of space used to store data with deduplication applied.  
In typical circumstances the amount of used space with deduplication applied is less than the amount of used space without deduplication applied.
- In the "Without dedupe" column: The amount of space that would be used to store data without deduplication applied.

### Free space

- In the "With dedupe" column: The amount of free space remaining in the volume with deduplication applied.  
In typical circumstances the amount of free space with deduplication applied is less than the amount of free space without deduplication applied.
- In the "Without dedupe" column: The amount of free space that would be remaining in the volume without deduplication applied.

### Snapshot overflow

The amount of space used for Snapshots in addition to the Snapshot reserved space in the selected volume.

### Snapshot reserve

The amount of Snapshot reserve space used in the selected volume.

### Total volume size

- In the "With dedupe" column: The total amount of used space in the selected volume.

- In the "Without dedupe" column: The total amount of logical space that would be used without deduplication applied.

In cases of over deduplication the logical total volume size might exceed the actual physical space allotted to the volume.

**Dedupe space saved** Displays numerical values for deduplication-related space savings.

<b>Used data space without dedupe</b>	The space that data would occupy on this volume without deduplication applied.
<b>Used data space with dedupe</b>	The space that data occupies on this volume with deduplication applied.
<b>Space saved</b>	The space that is saved on this volume because deduplication is applied.
<b>Space saved %</b>	The deduplication-enabled space saved expressed as a percentage of the logical total volume size.

**Dedupe properties** Displays the results of the last or current deduplication job run on the selected volume.

<b>Last run start time</b>	The time the last completed deduplication run started.
<b>Last run end time</b>	The time the last completed deduplication run ended.
<b>Current progress</b>	The progress of the current deduplication run or the time passed since the last deduplication run.
<b>Last run scan</b>	The amount of new data scanned for deduplication in the last deduplication run.
<b>Status</b>	The status of the current deduplication activity (idle or active)

## Exports tab

This tab displays information about the export settings applied to the selected dataset volume, LUN or qtree

**NFS Settings** Displays NFS export settings if NFS export is enabled for the selected dataset volume, or qtree.

**Anonymous users mapped to** Displays the port to which to map anonymous users.

**Do not allow UID option set** Displays whether or not the option to set the UID is enabled.

<b>Security settings</b>	Displays the types of security protocols assigned to the selected dataset member.
<b>All hosts</b>	Displays NFS permissions granted to all hosts.
<b>Specific Hosts</b>	Displays NFS permissions specific for each host name.
<b>Host</b>	Displays the name of the host for which specific NFS permissions are listed.
<b>CIFS Settings</b>	Displays CIFS export settings if CIFS export is enabled for the selected dataset volume, or qtree
<b>Windows Domain</b>	Displays the Windows Domain in which the selected volume is contained.
<b>User</b>	Displays the name of the user configured to access a CIFS share.
<b>Permission</b>	Displays specific permissions (full control, no access, or read and change) for specific users to access the nodes in this dataset
<b>FCP Settings</b>	Displays FCP export settings if FCP export is enabled for the selected dataset volume, LUN, or qtree
<b>The operating system</b>	The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
<b>The World Wide Port Names</b>	The world wide port names for the FC nodes if the accessing host does not have NetApp Host Agent installed
<b>iSCSI Settings</b>	Displays iSCSI export settings if iSCSI export is enabled for the selected dataset volume, LUN, or qtree
<b>Operating system</b>	The operating system (Solaris, Windows, HP-UX, AIX, Linux, VMware, NetWare) of the accessing host
<b>Initiator ID</b>	The initiator ID for the iSCSI nodes if the accessing host does not have a NetApp Host Agent installed

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.

- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Hosts > vFiler Units

---

You can use the **vFiler Units** window to view detailed information about vFiler units discovered by DataFabric Manager. From this window you can add vFiler units to or delete them from the NetApp Management Console host list. You can also access the Details tab, Paths tab, and the Relationships tabs for vFiler units.

- [Command buttons](#) on page 1023
- [vFiler units list](#) on page 1024
- [Details tab](#) on page 1026
- [Network Settings tab](#) on page 1027
- [Paths tab](#) on page 1028
- [Input Relationships tab](#) on page 1029
- [Output Relationships tab](#) on page 1029
- [Migration tab](#) on page 1030
- [Window customization](#) on page 1031

## Command buttons

The migration command buttons are disabled when a vFiler unit migration is in progress.

<b>Add</b>	Starts the <b>Add vFiler Unit</b> wizard, which allows you to create and to optionally configure vFiler units.  You can choose to create the vFiler unit by using the Add button and then configure it later by using the Setup button.
<b>Setup</b>	Starts the <b>Setup vFiler Unit</b> wizard, which allows you to configure or modify an existing vFiler unit.
<b>Delete</b>	Deletes the selected vFiler unit from the NetApp Management Console vFiler list.
<b>Start migration</b>	Initiates the first phase of a vFiler unit migration by starting the <b>vFiler Unit Migration</b> wizard, which begins a baseline transfer.
<b>Update</b>	Performs an on demand update of the SnapMirror relationships that were created as part of the "Start migration" operation. This button is enabled only when the "Start migration" operation has finished for the selected vFiler unit.
<b>Cutover</b>	Initiates the second phase of a migration, which performs a cutover (in other words, switches the source from the old storage from which the data is served to the new storage destination). This button is enabled only when the migration start operation has finished for the selected vFiler unit.

<b>Cancel</b>	Cancels the migration in progress for the selected dataset by stopping the migration process and returning the dataset to the status it had before the migration started. All ongoing data transfers for the migration are aborted, and the provisioned destination storage and destination vFiler unit are deleted. (You must manually delete VLANs and IPspaces that were created during the migration process.) This button is enabled during the migration start and update operations.
<b>Cleanup</b>	Initiates the third phase of a migration, which deletes the old storage from which the vFiler unit was migrated. A preview window lists which volumes are to be destroyed as part of the cleanup operation. VLANs and IPspaces used by the source vFiler unit are not automatically destroyed. This button is enabled only when a migration cutover process has finished for the selected vFiler unit.

## vFiler units list

<b>Name</b>	The name of the vFiler unit as it appears in the DataFabric Manager database.
<b>IP address</b>	The IP address associated with the selected vFiler unit.
<b>IP Space</b>	The name of the IPspace, if any, assigned to the vFiler unit.
<b>Hosting Storage System</b>	The name of the storage system that hosts the vFiler unit.
<b>System Status</b>	The current status of the vFiler unit. Possible values are Online, Offline, and Unknown. The default monitoring interval is five minutes. The interval is specified as the Ping Monitoring Interval in Operations Manager. You can use the Options page in Operations Manager to view or change the interval. See the Operations Manager online Help for details.
<b>Migration Status</b>	The status of a migrating source vFiler unit. The description, source storage status, destination storage status, permitted operations, and prohibited operations for each status are described as follows.  <b>Not started</b> The vFiler unit meets the vFiler unit migration requirements. <ul style="list-style-type: none"><li>• Source storage system: Online</li><li>• Destination storage : Not provisioned</li><li>• Operations permitted: All</li><li>• Prohibited operations: Migration cutover, migration update, migrate complete, migration cancel, migration cleanup</li></ul>

You can initialize the start migration operation on vFiler units having a "Not started" or "Migrate failed" status.

<b>In progress</b>	Migration of this vFiler unit has started.
	<ul style="list-style-type: none"> <li>• Source storage system: Online</li> <li>• Destination storage : Provisioned for the vFiler unit then offline</li> <li>• Operations permitted: Migration cancel</li> <li>• Prohibited operations: Add or delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies</li> </ul>
<b>Started, cutover required</b>	The vFiler unit is completely migrated to the destination storage system including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. The data source needs to be switched to the new vFiler unit on the new destination storage system.
	<ul style="list-style-type: none"> <li>• Source storage system: Offline</li> <li>• Destination storage: Online</li> <li>• Operations permitted: Edit provisioning or protection policies, migration update, migration cutover, migration cancel</li> <li>• Prohibited operations: Migration cleanup</li> </ul>
<b>Migrated, cleanup required</b>	The migration cutover operation is finished and the vFiler unit is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. Old storage needs to be deleted.
	<ul style="list-style-type: none"> <li>• Source storage system: Offline</li> <li>• Destination storage : Online</li> <li>• Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies, migration cleanup</li> <li>• Prohibited operations: Migration start, migration cancel, migration update, migration cutover</li> </ul>
<b>Migrated with errors</b>	The migration cutover operation successfully performed the switch to the destination storage system. However, a failure occurred during the migration of the backup version, backup relationships, or history for the primary data. You must manually correct the errors.
	<ul style="list-style-type: none"> <li>• Source storage system: Offline</li> <li>• Destination storage : Online</li> <li>• Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies</li> </ul>

- Prohibited operations: Migration start, migration cancel, migration update, migration cutover, migration cleanup

<b>Migrate failed</b>	The migration cutover operation failed to bring the destination vFiler unit online. The source vFiler unit is online again and the destination storage system is destroyed. <ul style="list-style-type: none"><li>• Source storage system: Online</li><li>• Destination storage : Offline</li><li>• Operations permitted: Resize storage, delete Snapshot copies, add and delete volumes, provision storage for the vFiler unit, edit provisioning or protection policies, migration start, migration cancel</li><li>• Prohibited operations: Migration cutover, migration cleanup, migration update</li></ul>
-----------------------	--

## Details tab

The Details tab has three areas: General, Service status, and Hosting Storage System Settings.

<b>General</b>	<b>Protocols</b>	Indicates the protocol type associated with the vFiler unit, either CIFS, NFS, or iSCSI.
<b>Mirrored</b>		Indicates whether the SnapMirror license is enabled on the hosting storage system. Possible values are Yes or No.
<b>Backup Destination</b>		Indicates whether a SnapVault Secondary license is enabled on this host, making the host a potential destination for backups. Possible values are Yes or No.
<b>Backup Source</b>		Indicates whether the SnapVault Data ONTAP Primary license is enabled on the hosting storage system, making the host a potential source of backups. Possible values are Yes or No. <b>Note:</b> Other hosts might also be potential backup sources, but the SnapVault Primary licenses for Linux, UNIX, and Windows are installed on the secondary system. This list confirms only whether the SnapVault Data ONTAP Primary license is enabled on the host.

<b>Service status</b>	<b>NFS</b>	Indicates whether the Network File System (NFS) service is Up or Down.
	<b>CIFS</b>	Indicates whether the Common Internet File System (CIFS) service is Up or Down.
	<b>iSCSI</b>	Indicates whether the iSCSI service is Up or Down.
<b>Hosting Storage System Settings</b>	These settings apply to the storage system that is hosting the vFiler unit that you selected in the vFiler list.	
	<b>Host Name</b>	The name that DataFabric Manager uses to log in to the storage system.
	<b>IP Address</b>	The IP address of the hosting storage system that is associated with the selected vFiler unit.
	<b>System Status</b>	Whether the status of the storage system is Online, Offline, or Unknown.
	<b>Login Credentials Status</b>	The current status of the login credentials that DataFabric Manager uses to log in to the hosting storage system. Possible values are Good, Bad, Read Only, Unknown, and Not Applicable.
	<b>NDMP Status</b>	<p>The Network Data Management Protocol (NDMP) availability of the storage system as of the most recent NDMP monitoring check.</p> <p>Possible values are Up, Down, and Unknown. The default interval for NDMP monitoring is 30 minutes.</p> <p>You can use the Backup Discovery Options page in Operations Manager to change the NDMP monitoring interval. See the Operations Manager online Help for instructions.</p>
	<b>NDMP Credentials Status</b>	<p>The current status of the Network Data Management Protocol credentials that DataFabric Manager uses to communicate with the hosting storage system.</p> <p>Possible values are Good, Bad, Unknown, and Not Applicable.</p> <p>You can use the NDMP Credentials page in Operations Manager to edit the credentials for NDMP discovery. See the Operations Manager online Help for details.</p>

## Network Settings tab

This tab provides information about vFiler unit administrative hosts and servers, and network bindings.

<b>Network information area</b>	This area displays information about administrative hosts and servers for a selected vFiler unit.
<b>Administrative host</b>	Indicates the IP address of the administrative host for the selected vFiler unit.
<b>DNS domain name</b>	Indicates the domain name of the DNS server for the selected vFiler unit.
<b>DNS servers</b>	Indicates the IP addresses of DNS servers for the selected vFiler unit.
<b>NIS domain name</b>	Indicates the domain name of the NIS server for the selected vFiler unit.
<b>NIS servers</b>	Indicates the IP addresses of NIS servers for the selected vFiler unit.
<b>CIFS authentication type</b>	Indicates the mode used to authenticate data requests to or from a selected vFiler unit. Values are Active directory or Windows workgroup.
<b>CIFS security style</b>	Indicates the security protocol to be used by a selected vFiler unit. Values are NTFS-only or Multiprotocol.
<b>CIFS workgroup name</b>	Indicates the name of the CIFS Windows workgroup.
<b>Network Bindings</b>	You can use network bindings to bind network cards, protocols, and services.
<b>IP address</b>	The IP address of a network card or port that you have bound to a specific protocol or service.
<b>Network mask</b>	The network mask of a network card or port that you have bound to a specific protocol or service.
<b>Network interface</b>	The protocol or service to which the corresponding IP address is bound.

## Paths tab

The Paths tab displays information about data that is moving into and out of host paths on the selected vFiler unit. You can use this information to identify dependencies on a selected vFiler unit, aggregate, volume, or qtree.

<b>Data coming into host path</b>	A list of locations from which data is being backed up or mirrored to the selected host path.
-----------------------------------	---

<b>Host path</b>	The host path for which incoming and outgoing data is shown for the storage system that is hosting the vFiler unit.
	You can view the flow of data into and out of the storage system as a whole, or you can expand the list to select a specific aggregate, volume, or qtree and view the flow of data through the selected path.
<b>Data coming out of host path</b>	A list of locations to which data is being backed up or mirrored from the selected host path.

### Input Relationships tab

This tab displays information about systems that send backup or mirror data to the storage system that is hosting the vFiler unit.

You can use this information to identify dependencies on a selected storage system before shutting down the system for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	The time elapsed since the last successful backup or mirror update.
<b>Source</b>	The location of the backup or mirror data that is being sent to the selected system.
<b>Type</b>	The type of relationship that the system has with the hosting storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	The name of the dataset to which the incoming data belongs.
<b>Destination</b>	The name of the hosting storage system on which the incoming data is being stored.

### Output Relationships tab

This tab displays information about systems that receive backup or mirror data from the hosting storage system.

You can use this information to identify dependencies on a selected storage system before shutting down the system for maintenance or to assess the impact of an outage.

<b>Lag Status</b>	Indicates whether the lag threshold specified for the relationship has been or is about to be exceeded.
<b>Lag</b>	The time elapsed since the last successful backup or mirror update.
<b>Source</b>	The location of data on the system that is being backed up or mirrored to a secondary system.

<b>Type</b>	The type of relationship the system has with the selected storage system. Possible values are SnapVault, Volume SnapMirror, or Qtree SnapMirror.
<b>Dataset</b>	The name of the dataset to which the outgoing data belongs.
<b>Destination</b>	The name of the destination system on which the outgoing data is being stored.

### Migration tab

This tab displays detailed information about the data migration of the datasets attached to the selected vFiler unit.

<b>Source storage system</b>	The name of the storage system from which the data is migrated.
<b>Destination storage system</b>	The name of the storage system into which the data is migrated.
<b>Migration Status</b>	The same migration status as in the vFiler units list section of this window.
<b>Dataset(s) attached</b>	The datasets to which the selected vFiler unit is attached.
<b>Physical resources</b>	The volumes in the dataset.
<b>Lag</b>	The length of time since the successful migration of data to the destination.
<b>Error</b>	The error that occurred during a migration operation. The value None indicates that no migration-related error occurred.
<b>State</b>	The state of the volume, SnapVault relationship, or SnapMirror relationship created during the migration.  <b>Uninitialized</b> The destination storage volume or qtree is not yet initialized or is being initialized.  <b>Snapvaulted</b> The SnapVault relationship is created and the qtree is a SnapVault secondary destination.  <b>Mirrored</b> The destination volume or qtree is in a SnapMirror relationship.  <b>Broken off</b> The destination was in a SnapMirror relationship, but a <code>snapmirror break</code> command made the volume or qtree writable.  This state is reported when the base Snapshot copy is still present in the volume. If the Snapshot copy is deleted, the state is reported as uninitialized while the destination is in the <code>/etc/snapmirror.conf</code> file. The <code>snapmirror resync</code> command restores the mirrored status.

<b>Quiesced</b>	SnapMirror is in a consistent internal state and no SnapMirror activity is occurring.
	In this state, you can create Snapshot copies with confidence that all destinations are consistent. The <code>snapmirror quiesce</code> command brings the destination into this state. The <code>snapmirror resume</code> command restarts all SnapMirror activities.
<b>Source</b>	A snapvault status or snapmirror status command was executed on the primary storage system.
	When the destination is on another storage system, its status is unknown and the provisioning application reports the status, "source." This status is also reported for SnapVault relationships when a <code>snapvault status</code> command is executed on secondary storage systems after the <code>snapvault restore</code> command was executed on an associated primary storage system.
<b>Unknown</b>	The destination volume or the volume that contains the destination qtree is in an unknown state.  It might be offline or restricted.
<b>Restoring</b>	SnapVault relationships are being restored.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries.  
Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify.  
The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.



# Data ► Datasets ► Overview

---

The **Datasets** window Overview tab provides a single location from which you can monitor the status of all datasets, create and modify datasets, and assign physical resources manually or by using provisioning policies. If you have the protection license, you can back up a dataset's content on demand, suspend or resume protection for it, and initiate restore operations to access backed-up data from this page.

- [Command buttons](#) on page 1033
- [Datasets list](#) on page 1034
- [Graph area](#) on page 1036
- [Details area](#) on page 1037
- [Window customization](#) on page 1039

## Command buttons

<b>Add</b>	Starts the <b>Add Dataset</b> wizard for adding a dataset.
<b>Edit</b>	Opens the <b>Edit Dataset</b> window, from which you can modify general properties of a dataset, physical resources of a dataset, or how storage is provisioned on a dataset.
<b>Delete</b>	Deletes the selected dataset and thereby removes the relationships among the storage resources.
<b>Protection Policy</b>	Starts the <b>Dataset Policy Change</b> wizard, from which you can select a protection policy and destination storage to associate with your dataset.
<b>Protect Now</b>	Opens the Protect Now dialog box, from which you can perform on-demand backup or mirror protection operations on datasets that are protection policy-enabled for those types of operations. This button is disabled for datasets that do not have a protection policy assigned.  If you click the box "Notify me on job progress," you receive desktop alerts about this job's status after starting the Protect Now process.  <b>Note:</b> With application datasets, clicking <b>Protect Now</b> copies all new backups that have not been copied to the secondary backup node. Protect Now does not create new local backups on the primary nodes of application datasets.
<b>Suspend</b>	Suspends dataset protection or provisioning for one or more datasets.  During the time that the application suspends protection, it displays a Protection Suspended status for the dataset.  This button is enabled only if a protection or provisioning policy is assigned to the dataset.

**Note:** When you click the Suspend button to stop the protection for an application dataset, a note displays, reminding you that local backups that are being created by another application cannot be suspended.

**Resume** Resumes dataset backup protection or provisioning for one or more datasets.

**Restore** Starts the **Restore** wizard for restoring backed-up copies of data.

## Datasets list

Lists information about existing datasets.

**Name** The name of the dataset.

**Overall Status** The status determined by evaluating the combined status conditions for disaster recovery, protection, conformance, space, and resources.

Licensing is checked before determining whether any status contributes to the overall status. If a feature is not licensed, it is not considered when determining the Overall Status value.

The following table shows how overall status is computed based upon other status values.

Overall Status	DR status condition	Protection status condition	Conformance status condition	Space status condition	Resource status condition
Error	Error	Lag error Baseline failed	Nonconformant	Error	Emergency Critical Error
Warning	Warning	Job failure Lag warning Uninitialized No protection policy for a non-empty dataset		Warning	Warning
Normal					

<b>Protection Policy</b>	The name of the protection policy currently assigned to the dataset.
<b>Primary Provisioning Policy</b>	The name of the provisioning policy currently assigned to the primary node of the dataset. If a provisioning policy is assigned to a secondary node in the dataset, that name is displayed in the details area when you select the secondary node in the graph area.
<b>Failed Over</b>	Indicates whether a disaster recovery-capable dataset has failed over. Valid values are the following:
<b>Yes</b>	Failover on the dataset was invoked and completed successfully, completed with warnings, or completed with errors.
<b>No</b>	Failover on the dataset has not been invoked.
<b>In Progress</b>	Failover on the dataset is currently in progress.
<b>Not Applicable</b>	The dataset is not assigned a disaster recovery protection policy and, therefore, is not capable of failover.
<b>Description</b>	A description of the dataset.
<b>Protection Status</b>	Displays protection status. This column is not shown by default and is not available if the protection application is not licensed.  Valid values, in alphabetical order, are as follows:
<b>Baseline Failed</b>	The dataset's initial baseline transfer did not succeed. Check the conformance status for more information.
<b>Initializing</b>	The dataset is in conforming state (becoming conformant) and its initial baseline transfer is taking place.
<b>Job Failure</b>	The most recent protection operation for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded the lag error threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.

<b>Lag Warning</b>	The dataset has reached or exceeded the lag warning threshold specified in the assigned protection policy.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>No Protection Policy</b>	The dataset is managed by the protection application, but no protection policy has been assigned to the dataset.
<b>Protected</b>	The data is being protected according to policy.
<b>Protection Suspended</b>	Protection for the dataset has been suspended.
<b>Uninitialized</b>	The dataset does not have any data in it, or it has only one node and its assigned policy has no schedule configured, or it has only one node and the backup Snapshot copy schedule for the assigned policy has not started any jobs.
<b>Space Status</b>	If you have the Provisioning license, displays the status of the available space for the selected dataset node (OK, Warning, Error, or Unknown). If any member of a dataset has space allocation error or warning conditions, the dataset's space status indicates that condition. You can select the dataset to scan its volumes, LUNs, or qtrees to determine which member is the cause of the warning or error condition. This item is not included in the dataset list by default.
<b>Conformance Status</b>	For the licensed protection application, indicates whether the dataset is Conformant, Nonconformant, or In Progress.
<b>Resource Status</b>	The most severe of all current events on all direct and indirect members of the dataset nodes. Values can be Emergency, Critical, Error, Warning, or Normal. This item is not included in the dataset list by default.
<b>Application</b>	The name of the application that created the application dataset, such as SnapManager for Oracle. This item is not included in the dataset list by default.
<b>Application Version</b>	The version of the application that created the application dataset. This item is not included in the dataset list by default.
<b>Application Server</b>	The name of the server that runs the application that created the application dataset. This item is not included in the dataset list by default.

### Graph area

The graphical representation of the nodes for the selected dataset are displayed in the lower section of the page. Click the node or connection on which you want to view status and configuration details.

## Details area

The details of the selected dataset node are displayed next to the graph area. Click  to view member details, status details, or resource details about the selected primary, secondary, or tertiary node.

<b>Primary data or Disaster recovery data node details</b>	If you select the Primary data node or the DR data node in the Graph area, the details area displays the following status and configuration information about the selected node.
<b>Protection</b>	Displays protection status. This item is not shown if the protection application is not licensed.  Valid values are as follows:
<b>Protected</b>	The data is being protected according to policy.
<b>No Protection Policy</b>	No protection policy is assigned to the dataset.
<b>Job Failure</b>	Protection for the dataset has failed.
<b>Lag Error</b>	The dataset has reached or exceeded a lag threshold.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag error period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>Lag Warning</b>	The dataset is approaching a lag threshold.  <b>Note:</b> This value indicates that there has been no successful backup or mirror copy of a node's data within a specified lag warning period. This condition is due either to backup or mirror copy failure, or to having no backup or mirror copy scheduled to fall within the specified period.
<b>Protection Suspended</b>	Protection for the dataset has been suspended.
<b>Uninitialized</b>	There are no backups for the dataset.
<b>Conformance</b>	For the licensed protection application, indicates whether the dataset is conformant. If a dataset is nonconformant, click  to evaluate errors and warnings and to run the conformance checker.

<b>Resource</b>	For the licensed protection application, represents the most severe of all current events on all direct and indirect members of the dataset nodes. Values can be Emergency, Critical, Error, Warning, or Normal. For Emergency, Critical, Error, or Warning conditions, click  to evaluate the events and sources causing those conditions.								
<b>Space</b>	For the licensed provisioning application, displays the status of the available space for the selected dataset node (OK, Warning, Error, or Unknown). If any volume, qtree, or LUN of a dataset has space allocation error or warning conditions, the dataset's space status indicates that condition. You can select the dataset to scan its volumes, LUNs, or qtrees to determine which member is the cause of the warning or error condition.								
<b>Failover</b>	Uses color, icons, and text to display the state and status of a dataset that is capable of disaster recovery. The colors and text vary according to the status of the activity. The state of a dataset can be Ready, Failing Over, or Failed Over. The status of an activity can be Normal, Warning, or Error.								
<b>Physical resources</b>	Displays the physical resources assigned to the selected dataset node. Click  for details.								
<b>Resource pools</b>	Displays the name of the resource pool. Click  for details.								
<b>Exports</b>	Displays information about the export settings applied to the selected dataset.								
<b>Local backup schedule</b>	Displays the name of the local backup schedule assigned to the protection policy of the selected dataset node.								
<b>Backup versions</b>	Lists local backups for a given dataset to help you select the files or directories to restore, or, if a volume has more backup versions than specified by its retention settings, which backup versions to delete.								
<b>Dataset properties details</b>	Depending on the properties of the selected dataset, the licensed protection application displays some or all of the following details. <table><tr><td><b>Owner</b></td><td>Owner of the current dataset.</td></tr><tr><td><b>Contact</b></td><td>E-mail contact address for this dataset.</td></tr><tr><td><b>Time zone</b></td><td>Time zone in which the dataset is located.</td></tr><tr><td><b>Application</b></td><td>(Displayed for application datasets) The application that generated the dataset.</td></tr></table>	<b>Owner</b>	Owner of the current dataset.	<b>Contact</b>	E-mail contact address for this dataset.	<b>Time zone</b>	Time zone in which the dataset is located.	<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.
<b>Owner</b>	Owner of the current dataset.								
<b>Contact</b>	E-mail contact address for this dataset.								
<b>Time zone</b>	Time zone in which the dataset is located.								
<b>Application</b>	(Displayed for application datasets) The application that generated the dataset.								

<b>Application version</b>	(Displayed for application datasets) The application version that generated the dataset.
<b>Application server</b>	(Displayed for application datasets) The name of the application server that generated the dataset.
<b>Connection details</b>	If you select a backup or mirror connection in the Graph area, the details area displays the following information about that connection:
<b>Relationships</b>	Displays the number of existing relationships for the selected connection. Click  for relationship details.
<b>Schedule</b>	Displays the name of the schedule that is assigned to the selected backup connection.
<b>Throttle</b>	Displays the name of the throttle schedule, if any, that is assigned to the selected connection.
<b>Lag status</b>	Displays the current lag status for the selected connection. If error or warning conditions exist, click  for details.
<b>Backup or Mirror node details</b>	If you select a Backup node or a Mirror node in the Graph area, the details area displays the following information about that node:
<b>Provisioning policy</b>	Lists the provisioning policies, if any, that are assigned to the selected node.
<b>Physical resources</b>	Lists the physical resources that are assigned to the selected node. Click  for details.
<b>Resource pools</b>	Lists the resource pools, if any, that are assigned to the selected node. Click  for details.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.
- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.

- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# Data ► Jobs

---

You can use the **Jobs** window to view status information for jobs initiated within NetApp Management Console .

- [Command button](#) on page 1041
- [View Jobs buttons](#) on page 1041
- [Jobs list](#) on page 1042
- [Completed Steps](#) on page 1045
- [Event description](#) on page 1045
- [Window customization](#) on page 1045

## Command button

**Cancel** Stops the selected jobs. You can select multiple jobs and cancel them simultaneously. This button is active only when the selected jobs are in progress.

## View Jobs buttons

These buttons specify the range of jobs displayed in the summary list.

**1 Day** Displays all jobs that were started between midnight of the previous day and now. (Jobs that were started before this period are not included even if they are still running.) This period can cover up to 47 hours and 59 minutes.

For example, if you click 1 Day at 15:00 on February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) on February 13 to the current time on February 14. This list covers the full day of February 13 plus the partial current day of February 14.

**1 Week** Displays all jobs that were started between midnight of the same day in the previous week (seven days ago) and now. (Jobs that were started before this period and are still running are not included.) This period can cover up to seven days, 23 hours, and 59 minutes.

For example, if you click 1 Week at 15:00 on Thursday, February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) the previous Thursday (February 7) to the current time on February 14. This list covers seven full days plus the partial current day.

**1 Month** Displays all jobs that were started between midnight of the same day in the previous month and now. (Jobs that were started before this period and are still running are not included.) This period can cover from 28 through 32 days, depending on the month.

For example, if you click 1 Month at 15:00 on Thursday, February 14 (on a 24-hour clock), the list includes all jobs that were started from 00:00 (midnight) on January 14 to the current time on February 14.

**All** Displays all jobs.

**Note:** On very large or very busy systems, the **Data > Jobs** window might be unresponsive for long periods while loading 1 Month or All data. If the application appears unresponsive for these large lists, select a shorter time period (such as 1 Day).

## Jobs list

Displays a list of the jobs that occurred. The list of jobs is updated dynamically, as jobs start or finish. You can customize the display using the filtering and sorting options in the jobs list.

**Note:** The lists of jobs that can be downloaded is limited to 25,000 records.

**Job Type** The type of job, which is determined by the policy assigned to the dataset or by the direct request initiated by a user. The default jobs list includes this column. The job types are as follows:

**Create relationship** A protection relationship create operation based on SnapMirror technology.

**Delete Snapshot copies** A job that deletes Snapshot copies of volumes of a dataset.

**Delete storage** A job that deletes a volume, qtree, or LUN from the storage system.

**Attention:** This operation will destroy the data in the deleted volume, qtree, or LUN. This operation cannot be reversed.

**Destroy relationship** A protection relationship delete operation based on SnapMirror technology.

**Failover** A dataset failover operation of a primary node to a disaster recovery node. Applies only if the dataset is enabled for disaster recovery.

**Local backup** A local scheduled backup protection operation based on Snapshot technology.

**Local backup confirmation** A local scheduled backup protection operation based on Snapshot technology. Applies if a dataset is an

	application-generated dataset and if the application is responsible for creating local backups.
<b>Mirror</b>	A scheduled protection mirror operation based on SnapMirror technology.
<b>On-demand protection</b>	A backup or mirror operation that is initiated by the Protect Now button in the <b>Datasets</b> window. The types of tasks performed are determined by the policy configured for the dataset.
<b>Provision</b>	A job that provisions containers into a dataset based on the associated policy and dataset attributes.
<b>Remote backup</b>	A scheduled backup to secondary storage based on SnapVault technology.
<b>Resize storage</b>	A job that changes the storage size or quota limit. If the selected container is a volume, this job type changes the size, Snapshot reserve, and maximum size of the volume. If the selected container is a qtree, this job type changes the quota limit of the qtree.
<b>Restore</b>	A protection data restore job that is initiated by the Restore button in the <b>Datasets</b> window.
<b>Dedupe volume</b>	A deduplication space savings operation initiated on a selected volume.
<b>Undedupe volume</b>	A deduplicated volume has been converted to a normal volume.
<b>Start migration</b>	A job that begins migrating a dataset or vFiler unit to a new storage system.
<b>Cancel migration</b>	A job that cancels a dataset or vFiler unit migration.
<b>Cleanup migration</b>	A job that deletes the old storage after a dataset or vFiler unit migration cutover.
<b>Cutover</b>	A job that switches the source of a dataset or vFiler unit from the old storage system to a new storage system.
<b>Migration update</b>	A job that updates the SnapMirror relationships that were created as part of the migration start operation.
<b>Relinquish migration</b>	A job that relinquishes the migration capability of a dataset.
<b>Dataset</b>	The name of the dataset on which the job was started. The default jobs list includes this column.

<b>vFiler Unit</b>	The name of the vFiler unit on which the job was started. The default jobs list includes this column if the provisioning license is installed.
<b>Start</b>	The date and time the job was started. The default jobs list includes this column.
<b>Job Status</b>	The running status of the job. The default jobs list includes this column. The progress options are as follows:
<b>Failed</b>	All tasks in the job failed.
<b>Partially Failed</b>	One or more of the tasks in the job failed and one or more of the tasks completed successfully.
<b>Succeeded</b>	All tasks completed successfully.
<b>Running</b>	The job is currently running.
<b>Running with Error</b>	The job is currently running but with an error.
<b>Queued</b>	The job is not running yet. However, it is scheduled to run after other provisioning jobs on the same dataset are completed.
<b>Canceled</b>	The job stopped because the Cancel button was clicked to stop the job before it was completed.
<b>Canceling</b>	The Cancel button was clicked and the job is in the process of stopping.
<b>End</b>	The date and time the job ended. The default jobs list includes this column.
<b>ID</b>	The identification number of the job.  The ID column is not displayed in the jobs list by default. The job identification number is unique and is assigned by the server when it starts the job. You can search for a particular job by entering the job identification number in the text box provided by the column filter.
<b>Bytes Transferred</b>	The amount of data (in megabytes or gigabytes) that was transferred during the job, as reported by DataFabric Manager. This column is not displayed in the jobs list by default.  <b>Note:</b> This number is an approximation and does not reflect an exact count; it is always less than the actual number of bytes transferred. For short jobs (jobs that take a short time to complete), no data transfer size is reported.
<b>Policy</b>	The name of the policy associated with the job. This column is not displayed in the jobs list by default.
<b>Source Node</b>	The name of the storage resource that contains the data being protected. This column is not displayed in the jobs list by default.

<b>Destination Node</b>	The name of the storage resource to which the data is transferred during the job. This column is not displayed in the jobs list by default.
<b>Submitted By</b>	The policy that automatically started the job or the user name of the person who started the job. This column is not displayed in the jobs list by default.
<b>Description</b>	A description of the job taken from the policy configuration or the job description entered when the job was manually started. This column is not displayed in the jobs list by default.

## Completed Steps

Displays detailed information about each task in the selected job. You can select a step to see its details.

<b>Time stamp</b>	The date and time the step was completed.
<b>Step</b>	A description of the step: for example, Start, in Progress, or End.
<b>Result</b>	The result of the step. Result options are as follows:
<b>Error</b>	The step failed.
<b>Warning</b>	The step succeeded but with a possible problem.
<b>Retry</b>	The provisioning engine has performed undo and retry operations.
<b>Normal</b>	The step succeeded.

## Event description

Displays detailed information about events and errors that occurred during each step of a job. The information displayed in this area includes much of the same information that is provided in the columns of the Details area. However, it also includes the unique items Job Description and Error Message.

To view the details, select an item from the jobs list, then select an item from the Completed Steps list.

## Window customization

You can modify the layout of the window by using a variety of customization options.

- You can use the sort arrow in the column header to specify the sort order of the entries. Click the column header to display the sort arrow.
- You can use the filter arrow  to display only the entries containing the information that you specify. The column heading is highlighted if a filter is applied.
- You can click the column display icon , located at the corner of the list, to select or deselect columns for viewing.

- You can drag the bottom of the datasets list area up or down to resize the main areas of the window.
- You can drag vertical dividers to resize the width of columns or other areas of the window.
- You can reorder columns in the list by dragging the column headers to another location.

# What groups are

---

A *group* is a collection of objects with common characteristics, such as location, project, or owning organization.

The groups you create in the licensed protection and provisioning applications are the same as the resource groups you create in Operations Manager. You can create single-type groups of objects, or you can create groups that include combinations of object types. You can create groups of objects such as datasets, resource pools, storage systems, hosts, vFiler units, aggregates, volumes, and qtrees. Objects can be members of more than one group.

Combining objects in groups allows you to filter data for the objects in the group. Grouping datasets and resource pools also enables you to see consolidated reports of information in Operations Manager. See the Operations Manager online help for detailed descriptions of the default views for datasets and resource pools and the custom catalogs you can use to create your own reports.

**Note:** If necessary, you can use Operations Manager to specify Storage Resource Management or chargeback settings or to create groups containing other types of objects (LUNs, SRM paths, and so on).

## Related concepts

[NetApp Management Console data filtering](#) on page 35

[Overview of resource pools](#) on page 819

[Dataset concepts](#) on page 693

[Dataset concepts](#) on page 693

[Overview of resource pools](#) on page 819

## Related tasks

[Changing dataset node resource assignments](#) on page 739



# Effect of time zones on schedules

---

Understanding how time zone settings can affect your protection schedules is important to be sure your backups and mirror copies are functioning as intended.

In Protection Manager, you determine the time zone to be used for a protection schedule when you set up your resource pools and your datasets. You have a choice of using the DataFabric Manager server's default time zone, creating a new default for datasets and resource pools, or selecting a different time zone each time you create or edit a dataset or resource pool in Protection Manager. The dataset contains your primary data and the resource pool contains destination storage that is available for provisioning to hold backups and mirror copies of your data.

Before selecting a schedule for a replication job, you need to know the time zones associated with the primary data and destination storage for that job. That information helps you determine when you want your local backups to occur, and when you want the remote replication to take place to achieve your data protection goals.

When the licensed protection application interprets a scheduled replication from primary data in a dataset to secondary destination storage, it uses the time zone of the primary data. When interpreting a scheduled replication from secondary storage to tertiary storage, the licensed protection application uses the time zone of the secondary node.

If you misapply time zones, unexpected and unwanted results could occur. For example, a weekly mirror copy to tertiary storage might occur before completion of the daily backup that you want to capture, or replication jobs might occur at a time of day when network bandwidth is already servicing a heavy load, and so forth.

**Note:** Some time zones observe daylight saving time (DST) and some do not. The licensed protection application automatically observes the local time zone and adjusts for daylight saving when appropriate. As a result, backups scheduled during the DST transition, between 1:00 am and 3:00 am local time, might not perform as intended.

## Next topics

[Ways to set the time zone](#) on page 274

[Guidelines for using time zones with resource pools](#) on page 276

[Guidelines for using time zones with datasets](#) on page 277

## Related concepts

[Decisions to make before adding datasets](#) on page 711

[Decisions to make before adding a resource pool](#) on page 837

[Impact of modifying resource pool properties](#) on page 843

[Dataset protection decisions](#) on page 711

[\*Protection schedules and time zones\*](#) on page 301

[\*Decisions to make before adding a protection policy\*](#) on page 251

[\*Planning schedules for protection policy nodes and connections\*](#) on page 293

#### **Related tasks**

[\*Adding a dataset\*](#) on page 719

[\*Adding a resource pool\*](#) on page 841

#### **Related references**

[\*Example of a schedule using local time zones\*](#) on page 279

[\*Example of a schedule using a default time zone\*](#) on page 283

# Protection policy node prerequisites

---

Before you attempt to implement a protection policy on your dataset nodes, ensure that the storage systems in the datasets or physical resource pools that make up that node meet the correct configuration and licensing requirements.

- Storage that is the source of a backup connection (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume, qtree, or OSSV directory if it is not an application dataset
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVault Data ONTAP Primary (for remote backup protection)
- Storage that is the source of a backup connection configured for nondisruptive LUN restore (to a NetApp storage system , not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume or qtree
    - A host, aggregate, or volume containing one of the above
  - Storage system licensing requires both of the following:
    - Data ONTAP Primary
    - Data ONTAP 7.3 or later
- Storage that is the source of a disaster recovery capable backup connection (to a NetApp storage system )
  - Configuration requirements are all of the following:
    - Qtree, volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes)
    - Dataset not configured for non-disruptive LUN restore
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a backup connection (Open System)
  - Configuration requirements: Open Systems SnapVault directory

- Storage system licensing requirements: Open Systems SnapVault client
- Storage that is the destination of a backup connection (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Volume
    - Qtree
    - Storage system or aggregate containing volumes and qtrees
  - Storage system licensing requirements are either of the following:
    - SnapMirror
    - SnapVaultData ONTAP Secondary (for remote backup protection)  
If the source is Windows, Linux, or UNIX, then SnapVault Windows, SnapVault Linux, or SnapVault UNIX is also required.
- Storage that is the destination of a backup connection configured for nondisruptive LUN restore (not disaster recovery capable)
  - Configuration requirements are either of the following:
    - Qtree or volume
    - Storage system or aggregate containing volumes and qtrees. Provisioning policy type (SAN or NAS) matches primary provisioning policy type or does not export storage.
  - Storage system licensing requirements are all of the following:
    - SnapVault
    - Data ONTAP Secondary
    - Data ONTAP 7.3 or later
- Storage that is the destination of a disaster recovery capable backup connection (to a disaster recovery node)
  - Configuration requirements:  
Volume (possibly containing qtrees), aggregate (possibly containing volumes) *or* an entire storage unit (possibly containing aggregates or volumes). No qtree on same storage system as the primary qtree. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a mirror connection (not disaster recovery capable)
  - Configuration requirements are any of the following:
    - Volume

- Qtree
  - Storage system, or aggregate, containing one of the above
  - Storage system licensing requirements: SnapMirror
- Storage that is the source of a disaster recovery capable mirror connection
    - Configuration requirements are all of the following:
      - Volume (possibly containing qtrees), aggregate (possibly containing volumes), *or* an entire storage unit (possibly containing aggregates or volumes)
      - Nothing that is in another dataset
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a mirror connection (not disaster recovery capable)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees
    - Storage system licensing requirements: SnapMirror
  - Storage that is the destination of a disaster recovery capable mirror connection (to a disaster recovery node)
    - Configuration requirements are any of the following:
      - Volume
      - Qtree
      - Storage system, aggregate, or volume containing volumes and qtrees. No volume on the same storage system as the primary volume. Provisioning policy type (SAN or NAS) matches primary provisioning policy type.
    - Storage system licensing requirements: SnapMirror
  - Any node
    - Configuration requirements: Nothing that is in a resource pool used by this dataset
    - Storage system licensing requirements: None
  - Primary (root) node with local backup schedule
    - Configuration requirements: No Open Systems SnapVault directories or Open Systems SnapVault hosts included
    - Storage system licensing requirements: None

- Non-root node
  - Configuration requirements: No Open Systems SnapVault directories or hosts and nothing that is in a non-root node of any other dataset and nothing that is in any node of this dataset.
  - Storage system licensing requirements: None

**Note:**

- If you plan to use SnapMirror with the licensed protection application, you must update the snapmirror.access option in Data ONTAP to specify the destination systems that are allowed to access the primary data source system.  
The snapmirror.access option specifies which SnapMirror destination systems can initiate transfers and which network interfaces they can use. For security reasons, the protection application does not modify the snapmirror.access option for you.
- A single storage system licensed as both SnapVault primary storage and SnapVault secondary storage locations cannot be included in a dataset.
- If you are restoring a LUN, the following points apply:
  - If the protection application is not configured to support non-disruptive LUN restore, the LUN in the destination location must be offline before you start the restore operation.
  - If the protection application is configured to support non-disruptive LUN restore, the LUN in the destination does not have to be offline unless it is owned by a vFiler unit.
  - If the destination LUN is owned by a vFiler unit, non-disruptive LUN restore is not supported.

**Related concepts**

[\*Decisions to make before adding datasets\*](#) on page 711

[\*Decisions to make before adding a resource pool\*](#) on page 837

[\*What a protection policy is\*](#) on page 847

# Administrator roles and capabilities

---

The administrator roles determine the tasks you can perform using applications in NetApp Management Console .

## Default and custom roles

One or more capabilities must be specified for every role, and you can assign multiple capabilities if you want the administrator to have more control than a specific role provides. For example, if you want an administrator to perform both the backup and restore operations, you must assign Back Up and Restore roles to the administrator.

The DataFabric Manager server and the client applications provide a set of default global roles described in the following list. You can customize these roles and the capabilities associated with them and you can create new ones using the Operations Manager Web-based user interface. For more information about configuring role-based access control (RBAC), see the *Operations Manager Administration Guide* .

<b>GlobalBackup</b>	You can initiate a backup to any secondary volume and ignore discovered hosts.
<b>GlobalDataProtection</b>	You can initiate a backup to any secondary volume; view backup configurations, events and alerts, and replication or failover policies; and import relationships into datasets.
<b>GlobalDataset</b>	You can create, modify, and delete datasets.
<b>GlobalDelete</b>	You can delete information in the DataFabric Manager server database, including groups and members of a group, monitored objects, custom views, primary and secondary storage systems, and backup relationships, schedules, and retention policies.
<b>GlobalEvent</b>	You can view, acknowledge, and delete events and alerts.
<b>GlobalFullControl</b>	You can view and perform any operation on any object in the DataFabric Manager server database and configure administrator accounts. You cannot apply this role to accounts with group access control.
<b>GlobalMirror</b>	You can create, destroy, and can update replication or failover policies.
<b>GlobalRead</b>	You can view the DataFabric Manager server database, backup and provisioning configurations, events and alerts, performance data, and policies.
<b>GlobalRestore</b>	You can restore the primary data back to a point in time or restore to a new location.
<b>GlobalWrite</b>	You can view or write to the DataFabric Manager server database.

<b>GlobalResourceControl</b>	You can add members to dataset nodes that are configured with provisioning policies.
<b>GlobalProvisioning</b>	You can provision primary dataset nodes and can attach resource pools to secondary or tertiary dataset nodes. The GlobalProvisioning role also includes all the capabilities of the GlobalResourceControl, GlobalRead, and GlobalDataset roles for dataset nodes that are configured with provisioning policies.
<b>GlobalPerfManagement</b>	You can manage views, event thresholds, and alarms apart from viewing performance information in Performance Advisor.

### Related concepts

[Strategies for enabling a dataset for migration](#) on page 779

### Related tasks

[Printing Help topics](#) on page 111

[Adding alarms](#) on page 601

[Testing alarms](#) on page 87

[Editing alarms](#) on page 89

[Deleting alarms](#) on page 91

[Responding to alarms](#) on page 95

[Monitoring alarms](#) on page 97

[Enabling and disabling alarms](#) on page 99

[Monitoring events](#) on page 65

[Responding to and acknowledging events](#) on page 67

[Deleting events](#) on page 69

[Adding a dataset](#) on page 719

[Assigning or changing a protection policy](#) on page 725

[Provisioning resources for a primary dataset node](#) on page 731

[Changing dataset node resource assignments](#) on page 739

[Adding resources to a dataset](#) on page 737

[Adding resources to a dataset](#) on page 737

[Changing dataset node resource assignments](#) on page 739

[Removing resources from a dataset](#) on page 741

[Editing dataset general properties](#) on page 753

[Deleting a dataset](#) on page 755

[Adding a resource pool](#) on page 841

[Editing resource pool properties](#) on page 845

[Adding groups](#) on page 461

[Editing groups](#) on page 463

[\*Deleting groups\*](#) on page 465  
[\*Adding a storage system\*](#) on page 915  
[\*Adding an Open Systems SnapVault host\*](#) on page 921  
[\*Adding a vFiler unit\*](#) on page 927  
[\*Setting up vFiler unit properties\*](#) on page 935  
[\*Editing storage system properties\*](#) on page 937  
[\*Editing Open Systems SnapVault properties\*](#) on page 939  
[\*Stopping Open Systems SnapVault agents\*](#) on page 941  
[\*Starting Open Systems SnapVault agents\*](#) on page 943  
[\*Updating Open Systems SnapVault client data\*](#) on page 945  
[\*Diagnosing a storage system\*](#) on page 947  
[\*Diagnosing an Open Systems SnapVault host\*](#) on page 949  
[\*Adding a daily protection schedule\*](#) on page 307  
[\*Adding a weekly protection schedule\*](#) on page 309  
[\*Adding a monthly protection schedule\*](#) on page 311  
[\*Adding a throttle schedule\*](#) on page 313  
[\*Deleting a protection or throttle schedule\*](#) on page 323  
[\*Assigning or changing schedules in a protection policy\*](#) on page 325  
[\*Copying a protection or throttle schedule\*](#) on page 327  
[\*Monitoring dataset status\*](#) on page 403  
[\*Monitoring backup and mirror relationships\*](#) on page 405  
[\*Backing up datasets on-demand\*](#) on page 407  
[\*Suspending protection of datasets\*](#) on page 409  
[\*Suspending data protection for backup volume maintenance\*](#) on page 411  
[\*Resuming protection of datasets\*](#) on page 413  
[\*Restoring backed-up data to a new location\*](#) on page 423  
[\*Restoring backed-up data over current data\*](#) on page 425  
[\*Restoring selected portions of a dataset\*](#) on page 427  
[\*Restoring a virtual machine to its original location\*](#) on page 429  
[\*Restoring a virtual machine file system to any location\*](#) on page 431  
[\*Restoring a virtual machine to its original location through another ESX server\*](#) on page 433  
[\*Importing discovered external relationships\*](#) on page 451  
[\*Adding unprotected host data to an existing dataset\*](#) on page 443  
[\*Adding unprotected host data to a new dataset\*](#) on page 445  
[\*Protecting unprotected datasets\*](#) on page 447  
[\*Starting a vFiler unit migration\*](#) on page 961  
[\*Updating vFiler unit migration SnapMirror relationships\*](#) on page 963  
[\*Cutting over to the new vFiler unit destination\*](#) on page 965  
[\*Cleaning up a vFiler unit migration\*](#) on page 967

- Cancelling a vFiler unit migration* on page 969
- Viewing vFiler unit migration status* on page 971
- Adding a protection policy* on page 671
- Editing a policy's primary data node* on page 258
- Editing a policy's backup connection* on page 259
- Editing a policy's backup node* on page 260
- Editing a policy's mirror connection* on page 260
- Editing a policy's mirror node* on page 261
- Changing retention times in a protection policy* on page 265
- Changing lag thresholds in a protection policy* on page 267
- Changing a node name in a policy* on page 269
- Deleting a protection policy* on page 271
- Editing a daily schedule* on page 315
- Editing a weekly schedule* on page 317
- Editing a monthly schedule* on page 319
- Editing a throttle schedule* on page 321
- Assigning or changing a provisioning policy* on page 727
- Configuring dataset nodes for NFS protocol access* on page 747
- Configuring dataset nodes for CIFS protocol access* on page 745
- Configuring dataset nodes for FC protocol access* on page 749
- Configuring dataset nodes for iSCSI protocol access* on page 751
- Displaying export properties for a specific dataset member* on page 417
- Displaying export and mapping information for all members of a dataset node* on page 415
- Monitoring failover readiness* on page 643
- Testing failover scripts* on page 644
- Updating disaster recovery node storage before failover* on page 646
- Starting failover* on page 647
- Monitoring failover status* on page 648
- Making the disaster recovery node the new primary data storage* on page 649
- Recovering by resuming forward mirroring* on page 651
- Recovering by resynchronizing data to undestroyed containers* on page 652
- Recovering by resynchronizing data to replaced containers* on page 654
- Testing failover scripts* on page 644
- Enabling disaster recovery protection* on page 641
- Adding a dataset* on page 719
  - Configuring dataset nodes for CIFS protocol access* on page 745
  - Configuring dataset nodes for NFS protocol access* on page 747
  - Configuring dataset nodes for iSCSI protocol access* on page 751
  - Configuring dataset nodes for FC protocol access* on page 749

*Assigning or changing a protection policy* on page 725  
*Provisioning resources for a primary dataset node* on page 731  
*Changing dataset node resource assignments* on page 739  
*Adding resources to a dataset* on page 737  
*Removing resources from a dataset* on page 741  
*Editing dataset general properties* on page 753  
*Deleting a dataset* on page 755  
*Viewing volume, LUN or qtree space allocation* on page 757  
*Diagnosing volume or qtree space status* on page 759  
*Diagnosing volume or qtree space status* on page 759  
*Resizing volume space* on page 761  
*Resizing qtree space* on page 763  
*Deleting Snapshot copies* on page 765  
*Deleting a volume, LUN or qtree* on page 767  
*Enabling deduplication on your dataset nodes* on page 809  
*Disabling deduplication on dataset nodes* on page 811  
*Starting on-demand deduplication* on page 813  
*Stopping an in-progress deduplication* on page 815  
*Viewing volume-level deduplication space-saving* on page 817  
*Adding a resource pool* on page 841  
*Editing resource pool properties* on page 845  
*Viewing a provisioning policy* on page 859  
*Adding a provisioning policy* on page 875  
*Editing a provisioning policy* on page 879  
*Copying a provisioning policy* on page 881  
*Deleting a provisioning policy* on page 883  
*Viewing vFiler templates* on page 889  
*Adding a vFiler template* on page 893  
*Editing a vFiler template* on page 895  
*Copying a vFiler template* on page 897  
*Deleting a vFiler template* on page 899  
*Adding a storage system* on page 915  
*Adding an Open Systems SnapVault host* on page 921  
*Adding a vFiler unit* on page 927  
*Setting up vFiler unit properties* on page 935  
*Editing storage system properties* on page 937  
*Editing Open Systems SnapVault properties* on page 939  
*Stopping Open Systems SnapVault agents* on page 941  
*Starting Open Systems SnapVault agents* on page 943

- Updating Open Systems SnapVault client data* on page 945
- Diagnosing a storage system* on page 947
- Diagnosing an Open Systems SnapVault host* on page 949
- Monitoring jobs* on page 973
- Cancelling jobs* on page 975
- Starting a dataset migration* on page 783
- Updating dataset migration SnapMirror relationships* on page 785
- Cutting over to the new dataset storage destination* on page 787
- Cleaning up a dataset migration* on page 789
- Relinquishing migration capability of a dataset* on page 797
- Cancelling a dataset migration* on page 791
- Viewing dataset migration status* on page 793
- Assigning or changing a provisioning policy* on page 727

#### **Related information**

*Operations Manager Administration Guide* -  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

# Index

## A

- access protocols
  - overview of configuring for [379, 743](#)
  - overview of support for [335, 699](#)
- active/active configurations
  - provisioning policy option [864](#)
- active/active hosts [165, 933](#)
- Add Alarm wizard
  - decisions to make [83](#)
  - task [85, 601](#)
- Add Dataset wizard
  - decisions to make [347, 711](#)
  - task [355, 673, 719](#)
- Add Group wizard
  - decisions to make [459](#)
  - task [461](#)
- Add OSSV Host wizard
  - decisions to make [149, 917](#)
  - task [153, 921](#)
- Add Protection Policy wizard
  - decisions to make [251](#)
  - task [255, 671](#)
- Add Provisioning Policy wizard
  - comparison to provisioning policy [851](#)
  - decisions to make [861](#)
  - task [875](#)
- Add Resource Pools wizard
  - decisions to make [223, 837](#)
  - task [227, 841](#)
- Add Schedule wizard
  - decisions to make [303](#)
  - task for daily [307](#)
  - task for monthly [311](#)
  - task for weekly [309](#)
- Add Storage System wizard
  - decisions to make [145, 913](#)
  - task [147, 915](#)
- Add vFiler Template wizard
  - decisions to make [891](#)
  - task [893](#)
- Add vFiler Unit wizard
  - decisions to make [155, 923](#)
  - task [159, 927](#)
- administrator roles
  - list of and descriptions [103, 603, 677, 1055](#)
- aggregates
  - on Data ONTAP 7.0 or earlier systems [217, 831](#)
  - resource pool guidelines [217, 831](#)
  - Unprotected Data window, Resources tab [521](#)
- alarms
  - adding [85, 601](#)
  - comparison to user alerts [73](#)
  - configuration guidelines for [77](#)
  - decisions to make before adding [83](#)
  - defined [71](#)
  - deleting [91](#)
  - disabling [99](#)
  - enabling [99](#)
  - list of monitoring and managing tasks for [93](#)
  - management tasks for, infrequent [94](#)
  - management tasks for, typical [93](#)
  - modifying [89](#)
  - monitoring [97](#)
  - pausing [99](#)
  - properties, described [79](#)
  - responding to [95](#)
  - testing [87](#)
  - triggered by related objects [75](#)
  - viewing [97](#)
- Alarms window [113, 563](#)
- alerts, comparison to alarms [73](#)
- application datasets
  - defined [123, 329, 693](#)
- applications in NetApp Management Console [29](#)

## B

- backup connections
  - description [237](#)
  - editing in a protection policy [259](#)
  - lag times [247](#)
  - planning a schedule assignment [294](#)
- backup nodes
  - changing resource assignments [371, 683, 735](#)
  - changing resources for [375, 739](#)
  - description [237](#)
  - editing in a protection policy [260](#)

backup nodes (*continued*)

selecting volumes for 213, 827

backup relationships

decisions to make before importing 449

enabling multiple 339, 703

implications of existing 441

importing 451

when to import 441

backup scripts, specifying for a primary data node 258

backups

of datasets on-demand 407

on Data ONTAP 7.0 or earlier 217, 831

suspending data protection for volume maintenance  
411

## C

CIFS data access protocol

configuring 381, 745

overview of configuring for 379, 743

overview of support for 335, 699

client platforms 27

Conform Now button 397

conformance

conditions for datasets 399

Conform Now button 397

Conformance Results window 397

dataset status, description of 395

datasets failure to conform 397

evaluating for datasets 397

how dataset conformance is monitored 397

monitor intervals 397

Preview Conformance button 397

conformance checking

suspending for the primary dataset node 409

Conformance Results window 397

console

adjusting column widths 33

applications supported 29

applications, toggling 31

filtering data display 35

Get Started feature 31

Help, accessing 31

logging out 31

moving backward and forward 31

rearranging column order 33

selecting columns to display 33

Tasks bar, hiding and redisplaying 33

credentials

login, editing for Open Systems SnapVault properties  
171, 939

login, editing for storage systems 169, 937

NDMP, editing for Open Systems SnapVault properties  
171, 939

NDMP, editing for storage systems 169, 937

custom name prefixes 352, 716

## D

daily backups

description of 242

scheduling 315

strategies for use 241

daily schedules

adding 307

definition 295

editing 315

dashboards

how to use 127, 687

panels, descriptions of 129, 689

dashboards, performance

described 127, 687

descriptions of panels 129, 689

dashboards, protection

Dataset Lags panel 485

Dataset Protection Status panel 479

described 127, 473, 687

descriptions of 129, 689

Failover Readiness panel 475, 665

Failover Status panel 477, 667

Protected Data panel 481

Resource Pools panel 989

Top Five Events panel 487, 987

Unprotected Data panel 483

dashboards, provisioning

Dataset Conformance Status panel 981

Dataset Resource Status panel 983

Dataset Space Status panel 991

described 127, 687, 979

descriptions of 129, 689

Resource Pool Space Status panel 985

Resource Pools panel 989

Top Five Events panel 487, 987

data 393, 419, 421, 423, 425, 431, 433, 435

See also unprotected data

protected, managing 393

restore overview 419

restoring a backed-up virtual machine 431

- data (*continued*)**
- restoring a virtual machine to its original location through another ESX server [433](#)
  - restoring backup to a new location [423](#)
  - restoring backup to current location [425](#)
  - restoring guidelines [421](#)
    - See also unprotected data
  - data access protocols**
    - overview of configuring for [379, 743](#)
    - overview of support for [335, 699](#)
  - Data Groups window** [509, 573](#)
  - Data Jobs window** [567, 1041](#)
  - Data ONTAP**
    - Data ONTAP 7.0, impact of [217, 831](#)
    - licenses, described [137, 905](#)
  - data protection**
    - backup compared to disaster recovery [579](#)
    - resuming for datasets [413](#)
    - suspending for backup volume maintenance [411](#)
    - suspending for datasets [409](#)
  - DataFabric Manager**
    - client [27](#)
    - Global group [455](#)
  - Dataset Conformance Status dashboard panel** [981](#)
  - Dataset Lags dashboard panel** [485](#)
  - dataset migration** [183, 187, 188, 189, 190, 342, 503, 621, 706, 769, 771, 773, 775, 777, 779, 781, 783, 785, 787, 789, 791, 793, 795, 797, 951, 955, 956, 957, 958](#)
    - See also vFiler unit migration
    - canceling [791](#)
    - configuring strategies [779](#)
    - decisions before starting [781](#)
    - deleting old storage [789](#)
    - description of tasks for [187, 955](#)
    - environment variables for scripts [795](#)
    - errors [187, 955](#)
    - failover interactions [773](#)
    - failures [187, 955](#)
    - how to view space utilization [342, 706](#)
    - limitations [775](#)
    - manual cleanup after migration [190, 958](#)
    - Migration tab, Datasets window [503](#)
    - overview for datasets [769](#)
    - relinquishing migration capability [621, 797](#)
    - requirements [771](#)
    - Step 1. Start
      - description [188, 956](#)
      - task [783](#)
    - dataset migration (*continued*)
      - Step 2. Update
        - description [188, 956](#)
        - task [785](#)
      - Step 3. Cutover
        - description [189, 957](#)
        - task [787](#)
      - Step 4. Cleanup
        - description [190, 958](#)
        - task [789](#)
      - viewing status [793](#)
      - when to relinquish migration capability [777](#)
        - See also vFiler unit migration
  - Dataset Migration wizard**
    - decisions to make [781](#)
    - task [783](#)
  - Dataset Policy Change wizard**
    - decisions to make [357, 721](#)
    - task [361, 675, 725](#)
  - Dataset Protection Status dashboard panel** [479](#)
  - Dataset Resource Status dashboard panel** [983](#)
  - Dataset Space Status dashboard panel** [991](#)
  - datasets**
    - adding [355, 673, 719](#)
    - adding resource assignments [371, 683, 735](#)
    - adding storage resources to [373, 737](#)
    - adding unprotected data to existing [443](#)
    - adding unprotected data to new [445](#)
    - adding, decisions to make for protection [348, 712](#)
    - adding, decisions to make for provisioning [350, 714](#)
    - assigning a protection policy [361, 675, 725](#)
    - assigning a provisioning policy [363, 727](#)
    - backing up on-demand [407](#)
    - changing resource assignments [371, 683, 735](#)
    - changing resources [375, 739](#)
    - concepts of [123, 329, 693](#)
    - configuring for disaster recovery [577](#)
    - configuring for migration [779](#)
    - conformance conditions [399](#)
    - conformance to policy, evaluating [397](#)
    - conformance to protection policies [331, 695](#)
    - conformance to provisioning policies [333, 697](#)
    - decisions before adding [347, 711](#)
    - decisions before importing discovered relationships [449](#)
    - decisions before provisioning [365, 729](#)
    - deleting [391, 755](#)
    - editing general properties [389, 753](#)
    - functionality [331, 695](#)
    - grouping [125, 453, 1047](#)

datasets (*continued*)

- how conformance is monitored 397
- importing discovered relationships into 451
- managing storage space, overview 341, 705
- managing storage space, tasks for 342, 706
- monitoring backup and mirror relationships 405
- monitoring conformance 981
- monitoring conformance to policy 397
- monitoring number of protected 481
- monitoring protection status 479
- monitoring resource status 983
- monitoring space status 991
- monitoring status 403
- monitoring status types 393
- names, acceptable characters 348, 712
- policies, decisions before changing 357, 721
- properties of 345, 709
- protecting unprotected data 447
- provisioning 333, 697
- provisioning resources for primary node 367, 731
- reasons for failure to conform to policy 397
- removing resources from 377, 741
- restoring portions of 427
- resuming protection of 413
- suspending protection of 409
- time zone guidelines 277
- time zones, effect on schedules 273, 1049
- types of conformance status, defined 395
- types of protection status, defined 394
- types of resource status, defined 395
- Unprotected Data window, aggregates 521
- Unprotected Data window, hosts 517
- Unprotected Data window, qtrees 525
- Unprotected Data window, volumes 523
- when to configure 337, 701
- when to manage storage space for 341, 705

Datasets tab

- Unprotected Data window 515
- Datasets window 489, 497, 503, 659, 1013, 1033
  - Current Space Breakout tab 1013
  - Disaster Recovery tab, Datasets window 497, 659
  - Migration tab 503
  - Overview tab 489, 1033
  - Provisioning tab 1013
  - Space Usage History tab 1013
- deduplication
  - about 619, 799
  - automated 619, 799
  - configuration requirements 801
  - disabling 811

deduplication (*continued*)

- enabling 809
- license, described 137, 905
- on-demand 619, 799
- over deduplication 805
- process overview 803
- scheduled 619, 799
- space savings percentage 807
- space savings, definition 807
- starting an on demand job 813
- stopping a job in progress 815
- support if the provisioning application is not licensed 593

Dependencies tab

- Protection Policies window, Overview tab 529
- Provisioning Policies window 997

Details tab

- OSSV (Open Systems SnapVault) window 545
- Provisioning Policies window 997
- Resource Pools window 511, 993
- Storage Systems Hosts window 537, 1005
- vFiler Units window 549, 1023

dfm option set timezone command 274

dfpm commands, inclusion in backup scripts 258

Diagnose OSSV Host wizard 181, 949

Diagnose Storage Systems wizard 179, 947

disaster recovery

- applying in a disaster situation 645
- assessing options 583, 645
- backups, comparison to 579
- by fallback to replaced containers 615, 654
- by fallback to undestroyed containers 611, 652
- configuring datasets for 577
- configuring, decisions to make 639
- dataset configuration decisions to make 639
- description of 623
- failover scripts, about 637
- failover scripts, example 638
- failover scripts, variables 637
- making the disaster recovery node the permanent primary data node 649
- overview of tasks 624
- protection policy-related decisions to make 640
- recovering after failover 585, 649
- relationship, definition of 625
- resuming forward mirroring 651
- starting failover 647
- stopping disaster recovery protection for all dataset members 391, 755
- strategies after failover 624

disaster recovery (*continued*)  
 updating before failover 646  
 volumes unsuitable as mirror destinations 633  
 when to use 623  
 disaster recovery capable  
 definition of 625  
 ensuring readiness 643  
 protection policies listed 609, 627  
 protection policy node requirements 243, 629, 1051  
 disaster recovery node  
 converting to permanent primary node 649  
 definition of 625  
 disaster recovery node storage  
 updating before failover 646  
 disaster recovery policies  
 decisions before applying to datasets 357, 721  
 discovered relationships  
 decisions to make before importing 449  
 importing 451  
 dpMaxFanInRatio option 339, 703

## E

environment variables for data migration scripts 795  
 ESX server guidelines  
 for adding or editing an Open Systems SnapVault host 151, 919  
 events  
 defined 39  
 deleting from event log 69  
 determining when they occur 41  
 Events window 117, 559  
 list of, complete 43  
 responding when an event occurs 67  
 severity types of 39  
 top five events in dashboard 487, 987  
 viewing the list of 65  
 where to find logs for 471, 977  
 export protocols  
 displaying for all members of a selected dataset node 415  
 displaying properties for specific dataset members 417  
 specifying for individual dataset members when provisioning a dataset 365, 729  
 external relationships  
 decisions to make before importing 449  
 importing 451  
 External Relationships tab  
 Unprotected Data window 527

## F

failback  
 to replaced containers 615, 654  
 to undestroyed containers 611, 652  
 failover  
 assessing the need for 583, 645  
 dashboard for monitoring readiness 475, 665  
 failover readiness, definition of 625  
 failover state, definition of 625  
 failover, definition of 625  
 monitoring readiness 643  
 monitoring status 648  
 process description 581, 635  
 scripts, testing 644  
 starting 647  
 updating disaster recovery node storage before 646  
 Failover Readiness dashboard panel 475, 665  
 failover scripts  
 definition of 625  
 description of 637  
 example of 638  
 invoked during the failover process 581, 635  
 variables in 637  
 failover status  
 dashboards for monitoring 477, 667  
 monitoring 648  
 Failover Status dashboard panel 477, 667  
 FC (Fibre Channel) data access protocol  
 configuring 385, 749  
 overview of configuring for 379, 743  
 overview of support for 335, 699  
 filtering data display 35  
 fractional reserve  
 about 871  
 and space management 869  
 FTP data access protocol, support for 335, 699  
 Full threshold 872

## G

Get Started feature 31  
 Global group 455  
 Graph tab  
 Datasets window, Disaster Recovery tab 497, 659  
 Protection Policies window, Overview tab 529  
 groups  
 adding 461  
 decisions to make before creating 459  
 defined 125, 453, 1047

## groups (*continued*)

- deleting 465
- editing 463
- filtering uses of 125, 453, 1047
- Global group 455
- impact of RBAC settings 461
- properties, described 457
- renaming 463

Groups window 509, 573

## H

### Help

- accessing 31
- printing topics 111

### hosts

- Data ONTAP licenses, described 137, 905
  - discovery by DataFabric Manager 133, 901
  - for unprotected data 439
  - investigating problems 135, 903
  - monitoring 133, 901
  - Open Systems SnapVault properties 545
  - storage system properties 537, 1005
  - Unprotected Data window, Resources tab 517
  - vFiler unit properties 549, 1023
  - visibility in protection application 133, 901
  - visibility in provisioning application 133, 901
- hourly backups
- description of 242
  - scheduling 315
  - strategies for use 241

## I

### Import Relationships wizard

- decisions to make 449
- task 451

### Input Relationships tab

- Storage Systems Hosts window 537, 1005
  - vFiler Units window 549, 1023
- iSCSI data access protocol
- configuring 387, 751
  - overview of configuring for 379, 743
  - overview of support for 335, 699

## J

### jobs

- cancelling 469, 975

## jobs (*continued*)

- monitoring 467, 973
- properties 567, 1041
- where to find logs for 471, 977

### Jobs tab

- Datasets window, Disaster Recovery tab 497, 659
- Jobs window 567, 1041

## L

### label

- resource pool, for filtering 221, 835

### lag times

- about 247
- assigning allowable limits on the mirror connection 260
- changing in a protection policy 267
- monitoring 485
- specifying acceptable limits for a backup connection 259

### licenses

- backup 141, 909
- described 137, 905
- NetApp Management Console applications 29

local time zone, example 279

logging out 31

### login credentials

- Open Systems SnapVault, editing 171, 939
- storage system, editing 169, 937

### logs

- for viewing the list of events 65
- where to find for jobs 471, 977

### LUNs

- deleting 767
- provisioning 333, 697
- viewing space allocation for 757

## M

maintenance, suspending data protection for backup volume 411

migration, See dataset migration

### Migration tab

- Datasets window 503
- vFiler Units window 549, 1023

### mirror connections

- description 237
- editing in a protection policy 260
- lag times 247
- planning a schedule assignment 294

mirror nodes  
 changing resource assignments 371, 683, 735  
 changing resources for 375, 739  
 description 237  
 selecting volumes for 215, 829

mirror protection  
 definition of 236  
 description 237

mirror relationships  
 decisions to make before importing 449  
 importing 451  
 on Data ONTAP 7.0 or earlier 217, 831

Monitor Events window 117, 559

monitoring  
 backup and mirror relationships 393  
 dashboard panels, overview of 129, 689  
 dashboards, overview of 127, 687  
 dataset conformance to policy 397  
 dataset status 393  
 events 65  
 protected data 393  
 protection dashboards 473  
 provisioning dashboards 979

monthly backups  
 description of 242  
 scheduling 319  
 strategies for use 241

monthly schedules  
 adding 311  
 definition 295  
 editing 319

MultiStore Option license, described 137, 905

## N

naming, custom prefixes 352, 716

NAS provisioning policies 863

NDMP credentials  
 diagnosing for Open Systems SnapVault host 181, 949  
 diagnosing for storage system 179, 947  
 Open Systems SnapVault, editing 171, 939  
 storage systems, editing 169, 937

NDMP status  
 diagnosing for a storage system 179, 947  
 diagnosing for Open Systems SnapVault host 181, 949

Nearly Full threshold 872

NearStore Option license, described 137, 905

NetApp Host Agent  
 diagnosing 181, 949  
 credentials, editing 171, 939

NetApp Host Agent (*continued*)  
 verifying presence in database 133, 901

NetApp Management Console 27, 29  
 See also console  
 applications supported 29  
 defined 27  
 See also console

Network Settings tab  
 vFiler Units window 549, 1023

NFS data access protocol  
 configuring 383, 747  
 overview of configuring for 379, 743  
 overview of support for 335, 699

Notifications Alarms window 113, 563

Notifications Events window 117, 559

## O

on-demand backup, datasets 407

Open Systems SnapVault  
 adding a host 153, 921  
 credentials, diagnosing 181, 949  
 decisions before adding host 149, 917  
 diagnosing problems 181, 949  
 guidelines for ESX servers 151, 919  
 investigating problems 135, 903  
 login credentials, editing 171, 939  
 NDMP status, diagnosing 181, 949  
 properties 545  
 properties, editing 171, 939  
 refreshing status data 177, 945  
 starting the agent 175, 943  
 stopping the agent 173, 941  
 updating client data 177, 945  
 verifying client presence in database 133, 901

Operations Manager  
 consolidated reports for 125, 453, 1047  
 logs, where to find 471, 977

OSSV (Open Systems SnapVault) Hosts window 545

OSSV, see Open Systems SnapVault 153, 921

Output Relationships tab  
 Storage Systems Hosts window 537, 1005  
 vFiler Units window 549, 1023

over deduplication 805

Overview tab  
 Datasets window 489, 1033  
 Protection Policies window 529

## P

### Paths tab

- OSSV (Open Systems SnapVault) window 545
- Storage Systems Hosts window 537, 1005
- vFiler Units window 549, 1023

### Performance Advisor

- application described 29

### plexes 866

### policies

- adding protection 255, 671
- adding provisioning 875
- definition of 599, 847
- evaluating dataset conformance to 397
- monitoring dataset conformance to 397
- protection, definition of 233, 847
- provisioning, definition of 848
- vFiler templates, definition of 597, 885

### Policies Provisioning window 997

### Preview Conformance button 397

### primary data components

- description 237

### primary data nodes

- about 237
- editing in a protection policy 258
- lag times 247
- planning a schedule assignment 293

### printing Help topics 111

### properties

- editing for datasets 389, 753
- impact of modifying resource pools 229, 843
- of alarms 113, 563
- of datasets 345, 709
- of datasets for protection 489, 1033
- of datasets with disaster recovery 497, 659
- of events 117, 559
- of groups 457, 509, 573
- of jobs 567, 1041
- of protection policies 529
- of protection policy schedules 535
- of provisioning policies 853
- of resource pools 511, 993
- of unprotected data, aggregates 521
- of unprotected data, hosts 517
- of unprotected data, qtrees 525
- of unprotected data, volumes 523
- of vFiler templates 887

Open Systems SnapVault, editing 171, 939

storage system, editing 169, 937

### protected data

- dataset conformance conditions 399
- dataset conformance status, described 395
- dataset protection status, described 394
- dataset resource status, described 395
- evaluating conformance to policy 397
- how dataset conformance is monitored 397
- managing, overview of 393
- reasons for failure to conform to policy 397
- restoring data 393
- resuming data protection 393
- suspending data protection 393

### Protected Data dashboard panel 481

### Protected dataset diagram, interpreting 361, 675, 725

### protection

- adding unprotected data to a dataset 443, 445
- dashboards, overview of 473
- decisions before adding a dataset 348, 712
- monitoring jobs for 467, 973
- of external relationships 451
- provisioning sequences 331, 695
- resuming dataset 413
- stopping protection for all dataset members 391, 755
- suspending for a dataset 409
- suspending for backup volume maintenance 411
- volumes unsuitable as mirror destinations 633

### Protection Dashboards window 473

### protection policies

- adding 255, 671
- assigning to datasets 361, 675, 725
- changing a node name 269
- changing lag time settings 267
- changing retention duration 265
- dataset dependencies on 529
- decisions before applying to datasets 357, 721
- decisions to make before adding 251
- definition of 233, 847
- deleting 271
- diagrams of 529
- disaster recovery capable, listing of 609, 627
- editing 257
- editing a backup connection 259
- editing a backup node 260
- editing a mirror connection 260
- editing a primary data node 258
- effects of time zone settings on schedule assignment 249, 301
- mirror protection 236
- node prerequisites 243, 629, 1051
- nodes and connections 237

protection policies (*continued*)  
 not disaster recovery capable, listed 239, 669  
 overview 123, 329, 693  
 Protection Policies window Overview tab 529  
 remote backup protection 235  
 retention classes 241, 242  
 retention strategies 241  
 schedules 535  
 types of data protection 235  
 when to configure 291  
 Protection Policies window Overview tab 529  
 Protection Policies window Schedules tab 535  
 provisioning  
   a specific aggregate or storage system 369, 733  
   adding a volume to a primary node 367, 731  
   comparision of policy and wizard 851  
   dashboards, overview of 979  
   decisions before 365, 729  
   decisions before adding a dataset 350, 714  
   monitoring jobs for 467, 973  
   Provisioning Manager, definition of 685  
   provisioning scripts for 873  
   working with datasets 333, 697  
 Provisioning Dashboards window 979  
 Provisioning Manager, definition of 685  
 provisioning policies  
   adding 875  
   assigning to datasets 363, 727  
   changing for a dataset 363, 727  
   comparision to provisioning wizard 851  
   copying 881  
   datasets rebaselining after changing policies 357, 721  
   decisions before applying to datasets 357, 721  
   decisions to make before adding 861  
   definition of 848  
   deleting 883  
   editing 879  
   editing, decisions to make before 877  
   overview 123, 329, 693  
   properties of 853  
 Provisioning Policies window 997  
 provisioning scripts 873  
 resource label, definition of 867  
 storage availability levels 864  
 types of 863  
 vFiler Templates window 1003  
 viewing 859  
 provisioning sequences  
   for backup destination volumes 213, 827  
   for mirror destination volumes 215, 829

Provisioning tab 1013  
 Provisioning wizard  
   decisions to make 365, 729  
   selecting a specific aggregate or storage system 369, 733  
   task 367, 731

## Q

Qtree SnapMirror, definition of 625  
 qtrees  
   deleting 767  
   provisioning 333, 697  
   provisioning by the protection application 331, 695  
   resizing 763  
   Unprotected Data window, Resources tab 525  
   viewing space allocation for 757

quotas  
   process 868  
   targets 868  
   types 868  
   why you use 867

## R

RAID-DP 865  
 RAID4 865  
 RBAC (role-based access control)  
   described 101  
   list of roles 103, 603, 677, 1055

rebaselining  
   about 357, 721  
   definition of 625

regular expressions, filtering examples 35

remote backups, defined 235

reports  
   in Operations Manager using groups 125, 453, 1047

resource labels  
   description of 867  
   how they work 221, 835

Resource Pool Space Status dashboard panel 985

resource pools  
   examples of 211, 825  
   adding 227, 841  
   advantages of using 207, 821  
   changing dataset assignment 375, 739  
   configuring 227, 841  
   decisions before adding 223, 837  
   decisions before changing assignments 371, 683, 735  
   defined 123, 329, 693

resource pools (*continued*)

- editing properties 231, 845
- editing, impact of 229, 843
- filtering 221, 835
- grouping 125, 453, 1047
- guidelines 217, 831
- labels for filtering 221, 835
- modifying properties 231, 845
- modifying, impact of 229, 843
- monitoring 989
- monitoring space status 985
- on Data ONTAP 7.0 or earlier systems 217, 831
- overview of 121, 205, 819
- properties 209, 823
- provisioning sequence for backups 213, 827
- provisioning sequence for mirrored copies 215, 829
- time zone guidelines 276
- time zone, effect on schedules 273, 1049

Resource Pools dashboard panel 989

Resource Pools window 511, 993

resource status, dataset 395

resources

- adding to datasets 373, 737
- removing from datasets 377, 741

Resources tab

- Unprotected Data window, aggregates button 521
- Unprotected Data window, hosts button 517
- Unprotected Data window, qtrees button 525
- Unprotected Data window, volumes button 523

restore

- enabling file overwrite and out-of-space warnings 419, 595
- guidelines for 421
- of a backed-up a virtual machine as files to any location 431
- of a virtual machine to original location 429
- of backed-up data over current data 425
- of backed-up data to new location 423
- portions of a dataset 427
- restore\_symboltable file 421
- restoring a virtual machine to its original location through another ESX server 433
- supported data operations, list of 419

Restore wizard

- a virtual machine file system to any location 431
- enabling file overwrite and out-of-space warnings 595
- guidelines 421
- restoring a virtual machine to its original location through another ESX server 433
- restoring backed-up data over current data 425

Restore wizard (*continued*)

- restoring backed-up data to a new location 423
- restoring portions of a dataset 427
- restoring virtual machine to current location 429
- retention
  - assigning duration on a backup node 260
  - assigning duration on a primary data node 258
  - changing duration in a protection policy 265
  - duration 242
  - of backups 241, 242
  - strategies 241
- roles, administrator (RBAC)
  - list of 103, 603, 677, 1055
  - RBAC described 101
- Rstorage availability levels 864

## S

SAN host

- provisioning for 369, 733

SAN provisioning policies 863

schedules

- adding daily 307
- adding monthly 311
- adding throttle 313
- adding weekly 309
- applying to a backup connection 294
- applying to policy nodes and connections 293
- assigning or switching in a protection policy 263, 325
- assigning to a backup connection 259
- assigning to a backup node 260
- assigning to a primary data node 258
- backup retention classes 241, 242
- baseline transfers in 331, 695
- copying 327
- decisions to make before creating 303
- deleting 323
- editing a throttle schedule 321
- editing daily 315
- editing monthly 319
- editing weekly 317
- features 289
- for throttling bandwidth 297
- overview 287
- planning for a mirror connection 294
- planning on a primary data node 293
- planning retention of backups 241
- time zones, effect on schedules 273, 1049
- when to configure 291

Schedules tab, Protection Policies window 535

- secondary provisioning policies 863
  - Set Up Alarms window 113, 563
  - Setup vFiler Unit wizard
    - decisions to make 161, 929
    - task 167, 935
  - severity types for events 39
  - SnapMirror
    - for backups 141, 909
    - license, described 137, 905
  - SnapMirror relationship break
    - definition of 625
    - invoked during the failover process 581, 635
  - SnapMirror relationships
    - updating during dataset migration 785
    - updating during vFiler unit migration 195, 963
  - SnapMirror Sync
    - license, described 137, 905
  - Snapshot copies
    - deleting 765
    - overview of storage space management 341, 705
    - reallocating space for in a volume 761
  - SnapVault
    - for backups 141, 909
    - Primary license, described 137, 905
    - provisioning sequence for backups 213, 827
    - provisioning sequence for mirrored copies 215, 829
    - Secondary license, described 137, 905
    - Windows Open File Manager license, described 137, 905
  - SnapVault Linux
    - license, described 137, 905
  - SnapVault Unix
    - license, described 137, 905
  - Space Breakout tab, Resource Pools window 511, 993
  - space guarantees
    - about 869
    - space management option 869
  - space management
    - deleting Snapshot copies 765
    - deleting volumes, LUNs, and qtrees 767
    - description of 341, 705
    - diagnosing space status 759
    - how it works 869
    - how to view space utilization 342, 706
    - overview of resize options 343, 707
    - reallocating volume space 761
    - resizing qtree space 763
    - space utilization thresholds 872
    - task overview 342, 706
    - viewing space allocations 757
  - space management (*continued*)
    - when to use 341, 705
  - space reservations
    - about 870
    - space management option 869
  - status definitions, dataset
    - conformance 395
    - protection 394, 395
  - storage systems
    - adding 147, 915
    - credentials, diagnosing 179, 947
    - Data ONTAP licenses, described 137, 905
    - decisions before adding 145, 913
    - diagnosing 179, 947
    - investigating problems 135, 903
    - licenses, diagnosing 179, 947
    - login credentials 169, 937
    - NDMP credentials 169, 937
    - NDMP status, diagnosing 179, 947
    - properties 537, 1005
    - properties, editing 169, 937
    - verifying presence in database 133, 901
    - viewing interdependencies 135, 903
  - Storage Systems Hosts window 537, 1005
  - SyncMirror
    - advantages 866
    - description of 866
    - provisioning policy option 864
  - syslog cluster messages, where to find 471, 977
- ## T
- Tasks bar, hiding and redisplaying 33
  - thresholds
    - for space utilization 872
  - throttle schedules
    - adding 313
    - definition 297
    - editing 321
  - time zones
    - effect on schedules 273, 1049
    - effects on schedule execution 249, 301
    - example using default value 283
    - example using local time 279
    - guidelines with datasets 277
    - guidelines with resource pools 276
    - setting in DataFabric Manager 274
    - setting in Protection Manager 274
    - setting the default 274
    - system default 274

time zones (*continued*)

understanding 273, 1049

Top Five Events dashboard panel 487, 987

troubleshooting

dataset conformance conditions 399

datasets fail to conform 397

evaluating dataset conformance 397

restore\_symboltable file 421

## U

unprotected data

adding to a new dataset 445

adding to an existing dataset 443

assigning a protection policy 361, 675, 725

decisions to make before importing 449

definition of 435

hosts for 439

importing discovered relationships 451

monitoring 483

protecting 447

when to import discovered relationships 441

where to view details about 437

Unprotected Data dashboard panel 483

Unprotected Data window

Datasets tab 515

External Relationships tab 527

Resources tab, aggregates button 521

Resources tab, hosts button 517

Resources tab, qtrees button 525

Resources tab, volumes button 523

update operation

assessing the need before failover 583, 645

Usage tab

Storage Systems Hosts window 537, 1005

user alerts, comparison to alarms 73

## V

vFiler templates

adding 893

copying 897

decisions before adding 891

definition of 597, 885

deleting 899

editing 895

properties of 887

viewing 889

vFiler Templates window 1003

vFiler unit migration 183, 185, 187, 188, 189, 190, 191, 193, 195, 197, 199, 201, 203, 769, 795, 951, 953, 955, 956, 957, 958, 959, 961, 963, 965, 967, 969, 971

See also dataset migration

canceling 201, 969

decisions before starting 191, 959

deleting old storage 199, 967

description of tasks for 187, 955

environment variables for scripts 795

errors 187, 955

failures 187, 955

manual cleanup after migration 190, 958

overview 183, 951

requirements 185, 953

Step 1. Start

description 188, 956

task 193, 961

Step 2. Update

description 188, 956

task 195, 963

Step 3. Cutover

description 189, 957

task 197, 965

Step 4. Cleanup

description 190, 958

task 199, 967

viewing status 203, 971

See also dataset migration

vFiler unit Migration wizard

decisions to make 191, 959

task 193, 961

vFiler units

active/active hosts 165, 933

adding 159, 927

decisions before adding unit 155, 923

decisions before setting up properties 161, 929

investigating problems 135, 903

properties 549, 1023

setting up properties for 167, 935

template window for 1003

using a script to customize 143, 911

verifying presence in database 133, 901

vFiler Units Hosts window 549, 1023

virtual machine

restoring file system to any location 431

restoring to original location 429

restoring to original location thru ESX server 433

VMware ESX server

guidelines 151, 919

**Volume SnapMirror**

definition of [625](#)

**volumes**

adding to primary node [367, 731](#)

deleting [767](#)

deleting Snapshot copies [765](#)

maximum number supported [861](#)

provisioning [333, 697](#)

provisioning by the protection application [331, 695](#)

resizing [341, 705, 761](#)

suspending data protection for backup maintenance

[411](#)

Unprotected Data window, Resources tab [523](#)

viewing space allocation for [341, 705, 757](#)

**W**

WebDev data access protocol, support for [335, 699](#)

**weekly backups**

description of [242](#)

scheduling [317](#)

strategies for use [241](#)

**weekly schedules**

adding [309](#)

definition [295](#)

editing [317](#)

