



SnapDrive for UNIX configuration

Snapdrive for Unix

NetApp
March 24, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapdrive-unix/aix/concept_what_the_snapdrive_conf_file_is.html on March 24, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- SnapDrive for UNIX configuration 1
 - Configuring SnapDrive for UNIX 1
 - Configuration information for Vserver 34
 - Audit, recovery, and trace logging in SnapDrive for UNIX 36
 - What AutoSupport is 42
 - Support for multipath access in SnapDrive for UNIX 45
 - Thin provisioning in SnapDrive for UNIX 49
 - Multiple subnet configuration 50
 - Automatic detection of host entities 53
 - What SnapDrive wizards are 58

SnapDrive for UNIX configuration

You must know the SnapDrive for UNIX configuration options and understand how to use SnapDrive for UNIX.

Configuring SnapDrive for UNIX

You can edit the `snapdrive.conf` file, which contains all the configuration variables and options used in SnapDrive for UNIX, to enable or disable options according to your requirements. You can also add variables to create host-specific usage.

What the `snapdrive.conf` file is

The `snapdrive.conf` file contains a name-value pair for each configurable variable that SnapDrive for UNIX use to function. SnapDrive for UNIX automatically checks the information in this file each time it starts. You can use a text editor to modify this file.

The `snapdrive.conf` file is located in the SnapDrive installation directory. The `snapdrive config show` command displays the current and active contents of the `snapdrive.conf` file.

Configuration options and their default values




You can determine the current configurable variables and their settings by running the `snapdrive config show` command.


The supported configurable items and their default settings can vary across host operating systems and the different versions of SnapDrive for UNIX. For example, on AIX the default path is `/var/log/...`

The following table describes the parameters in the `snapdrive.conf` file:

Variable	Description
<code>lunpath-monitor-frequency</code>	Enables you to specify how often SnapDrive for UNIX automatically fixes LUN paths. The default value is 24 hours.

Variable	Description
<code>blacklist-interfaces</code>	<p>Enables you to specify, when there are multiple Ethernet interfaces, the interfaces that you do not want to use, to reduce operation time. If the configuration has multiple Ethernet interfaces, SnapDrive for UNIX at times searches through the list of interfaces to determine if the interface can ping. If the interface fails to ping, it tries for five times before checking the next interface. Thus, the operation takes additional time to execute.</p> <p>If you want SnapDrive to ignore some of the interfaces, you can specify those interfaces in the <code>blacklist-interfaces</code> parameter. This reduces the operation time.</p>
<code>all-access-if-rbac-unspecified=on</code>	<p>Specifies the access-control permissions for each host on which SnapDrive for UNIX runs by entering the permission string in an access-control file. The string that you specify controls which SnapDrive for UNIX Snapshot copy and other storage operations a host might perform on a storage system. (These access permissions do not affect the show or list operations.)</p> <p>Set this value to either <code>on</code> or <code>off</code> where:</p> <ul style="list-style-type: none"> • <code>on</code> specifies that SnapDrive for UNIX enables all access permissions if no access-control permissions file exists on the storage system. The default value is <code>on</code>. • <code>off</code> specifies that the storage system allows the host only the permissions that are mentioned in the access-control permissions file. <p>If you provide an access-control file, this option has no effect.</p>
<code>allow-partial-clone-connect=on</code>	<p>SnapDrive for UNIX enables you to connect to a subset of file systems or only to the host volume of the cloned disk group.</p> <p>Set this value to <code>on</code> or <code>off</code>:</p> <ul style="list-style-type: none"> • <code>on</code> specifies that SnapDrive for UNIX enables you to connect to a subset of file systems or only to the host volume of the cloned disk group. • <code>off</code> determines that SnapDrive for UNIX cannot connect to a subset of file systems or only to the host volume of the cloned disk group.



Variable	Description
<code>audit-log-file="/var/log/sd-audit.log"</code>	<p>Specifies the location where SnapDrive for UNIX writes the audit log file.</p> <p>The default value depends on your host operating system. The path shown in the example is the default path for a AIX host.</p>
<code>audit-log-max-size=20480</code>	<p>Specifies the maximum size, in bytes, of the audit log file. When the file reaches this size, SnapDrive for UNIX renames it and starts a new audit log. The default value is <code>20480</code> bytes. Because SnapDrive for UNIX never starts a new log file in the middle of an operation, the correct size of the file could vary slightly from the value specified here.</p> <div data-bbox="865 762 930 825" style="float: left; margin-right: 10px;">  </div> <div data-bbox="1005 695 1461 894" style="border: 1px solid #ccc; padding: 10px; margin-left: 20px;"> <p>You should use the default value. If you decide to change the default value, remember that too many log files can take up space on your disk and might eventually affect performance.</p> </div>
<code>audit-log-save=2</code>	<p>Determines how many old audit log files SnapDrive for UNIX should save. After this limit is reached, SnapDrive for UNIX discards the oldest file and creates a new one.</p> <p>SnapDrive for UNIX rotates this file based on the value you specify in the <code>audit-log-save</code> variable. The default value is <code>2</code>.</p> <div data-bbox="865 1346 930 1409" style="float: left; margin-right: 10px;">  </div> <div data-bbox="1005 1276 1461 1476" style="border: 1px solid #ccc; padding: 10px; margin-left: 20px;"> <p>You should use the default value. If you decide to change the default value, remember that too many log files can take up space on your disk and might eventually affect performance.</p> </div>
<code>autosupport-enabled</code>	<p>Determines that the option <code>autosupport-enabled</code> is <code>on</code> by default.</p> <p>This option is enabled by default to store the AutoSupport information in the Event Management System (EMS) log of the storage system.</p> <div data-bbox="865 1808 930 1871" style="float: left; margin-right: 10px;">  </div> <div data-bbox="1005 1791 1461 1892" style="border: 1px solid #ccc; padding: 10px; margin-left: 20px;"> <p>SnapDrive 4.2 for UNIX and later versions do not have the option <code>autosupport-filer</code>.</p> </div>


Variable	Description
<code>available-lun-reserve=8</code>	<p>Specifies the number of LUNs that the host must be prepared to create when the current SnapDrive for UNIX operation completes. If few operating system resources are available to create the number of LUNs specified, SnapDrive for UNIX requests additional resources, based on the value supplied in the <code>enable-implicit-host-preparation</code> variable.</p> <p>The default value is 8.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>This variable applies only to systems that require host preparation before you can create LUNs. Hosts require this preparation.</p> <p>This variable is used on configurations that include LUNs.</p> </div>
<code>bypass-snapdrive-clone-generated-check</code>	<p>Specifies that the deletion of the SnapDrive generated or Non-snapdrive generated FlexClone.</p> <p>Set this value to either <code>on</code> or <code>off</code> where:</p> <ul style="list-style-type: none"> • <code>on</code> - Specifies that SnapDrive for UNIX allows to delete the FlexClone volume of the snapdrive-generated and non-snapdrive generated FlexClone. • <code>off</code> - Specifies that SnapDrive for UNIX allows to delete only the FlexClone volume of the snapdrive-generated. The default value is <code>off</code>.


Variable	Description
<code>check-export-permission-nfs-clone</code>	<p>Determines that setting the NFS export permission allows/disables to create cloning in the secondary host (host which does not have export permissions on the parent volume) or storage system.</p> <ul style="list-style-type: none">• <code>on</code> - SnapDrive for UNIX checks for appropriate export permission on the volume for the secondary host. The default value is <code>on</code>.• <code>off</code> - SnapDrive for UNIX does not check appropriate export permission on the volume for the secondary host. <p>SnapDrive for UNIX does not allow cloning if there is no export permission for a volume in an NFS entity. To overcome this situation, disable this variable in the <code>snapdrive.conf</code> file. As a result of the cloning operation, SnapDrive provides appropriate access permissions on the cloned volume.</p> <p>Setting the value to <code>off</code> enables secondary protection to work in clustered Data ONTAP.</p>

Variable	Description
<code>cluster-operation-timeout-secs=600</code>	<p>Specifies the host cluster operation timeout, in seconds. You should set this value when working with remote nodes and HA pair operations to determine when the SnapDrive for UNIX operation should time out. The default value is <code>600</code> seconds.</p> <p>Other than the non-master node, the host cluster master node can also be the remote node, if the SnapDrive for UNIX operation is initiated from a non-master node.</p> <p>If SnapDrive for UNIX operations on any node in the host cluster exceed the value you set, or the default of <code>600</code> seconds (if you set no value), the operation times out with the following message:</p> <div data-bbox="820 703 1485 1243" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>Remote Execution of command on slave node sfrac-57 timed out. Possible reason could be that timeout is too less for that system. You can increase the cluster connect timeout in snapdrive.conf file. Please do the necessary cleanup manually. Also, please check the operation can be restricted to lesser jobs to be done so that time required is reduced.</pre> </div>
<code>contact-http-port=80</code>	<p>Specifies the HTTP port to use for communicating with a storage system. The default value is <code>80</code>.</p>
<code>contact-ssl-port=443</code>	<p>Specifies the SSL port to use for communicating with a storage system. The default value is <code>443</code>.</p>
<code>contact-http-port-sdu-daemon=4094</code>	<p>Specifies the HTTP port to use for communicating with the SnapDrive for UNIX daemon. The default value is <code>4094</code>.</p>
<code>contact-http-dfm-port=8088</code>	<p>Specifies the HTTP port to use for communicating with an Operations Manager server. The default value is <code>8088</code>.</p>

Variable	Description
<code>contact-ssl-dfm-port=8488</code>	Specifies the SSL port to use for communicating with an Operations Manager server. The default value is <code>8488</code> .
<code>datamotion-cutover-wait=120</code>	Specifies the number of seconds SnapDrive for UNIX waits for the DataMotion for vFiler (cutover phase) operations to complete and then retries the SnapDrive for UNIX commands. The default value is <code>120</code> seconds.
<code>dfm-api-timeout=180</code>	Specifies the number of seconds SnapDrive for UNIX waits for the DFM API to return. The default value is <code>180</code> seconds.
<code>dfm-rbac-retries=12</code>	Specifies the number of times SnapDrive for UNIX checks access retries for an Operations Manager refresh. The default value is <code>12</code> .
<code>dfm-rbac-retry-sleep-secs=15</code>	Specifies the number of seconds SnapDrive for UNIX waits before retrying an access check for an Operations Manager refresh. The default value is <code>15</code> .
<code>default-noprompt=off</code>	Specify if you want the <code>-noprompt</code> option to be available. The default value is <code>off</code> (not available). If you change this option to <code>on</code> SnapDrive for UNIX does not prompt you to confirm an action requested by <code>-force</code> .

Variable	Description
<code>device-retries=3</code>	<p>Specifies the number of inquiries that the SnapDrive for UNIX can make about the device where the LUN resides. The default value is 3.</p> <p>In normal circumstances, the default value should be adequate. In other circumstances, LUN queries for a snap create operation could fail because the storage system is exceptionally busy.</p> <p>If the LUN queries keep failing even though the LUNs are online and correctly configured, you might want to increase the number of retries.</p> <p>This variable is used on configurations that include LUNs.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>You should configure the same value for the <code>device-retries</code> variable across all the nodes in the host cluster. Otherwise, the device discovery involving multiple host cluster nodes can fail on some nodes and succeed on others.</p> </div>
<code>device-retry-sleep-secs=1</code>	<p>Specifies the number of seconds SnapDrive for UNIX waits between inquiries about the device where the LUN resides. The default value is 1 second.</p> <p>In normal circumstances, the default value should be adequate. In other circumstances, LUN queries for a snap create operation could fail because the storage system is exceptionally busy.</p> <p>If the LUN queries keep failing even though the LUNs are online and correctly configured, you might want to increase the number of seconds between retries.</p> <p>This variable is used on configurations that include LUNs.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>You should configure the same value for the <code>device-retry-sleep-secs</code> option across all the nodes in the host cluster. Otherwise, the device discovery involving multiple host cluster nodes can fail on some nodes and succeed on others.</p> </div>

Variable	Description
<pre>default-transport=iscsi</pre>	<p>Specifies the protocol that SnapDrive for UNIX uses as the transport type when creating storage, if a decision is required. The acceptable values are <code>iscsi</code> or <code>FCP</code>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>If a host is configured for only one type of transport and that type is supported by SnapDrive for UNIX, SnapDrive for UNIX uses that transport type, irrespective of the type specified in the <code>snapdrive.conf</code> file.</p> </div> <p>On AIX hosts, ensure the <code>multipathing-type</code> option is set correctly. If you specify <code>FCP</code>, you must set <code>multipathing-type</code> to one of the following values:</p> <ul style="list-style-type: none"> • <code>NativeMPIO</code> • <code>DMP</code>
<pre>enable-alu=on</pre>	<p>Determines that the ALUA is supported for multipathing on the igroup. The storage systems must be HA pair and the HA pair failover state in <code>single-image</code> mode.</p> <ul style="list-style-type: none"> • The default value is <code>on</code> to support ALUA for igroup • You can disable the ALUA support by setting the option <code>off</code>
<pre>enable-fcp-cache=on</pre>	<p>Specifies whether to enable or disable the cache. SnapDrive maintains a cache of available active ports and the port names (WWPNs) information to send the response faster.</p> <p>This variable is useful in few scenario where there is no FC cables connected to the port or wrap plug is used in the port, SnapDrive for UNIX may experience long delays to fetch the information about FC interface and their corresponding WWPNs. The caching helps to resolve/improve the performance of SnapDrive operations in such environments.</p> <p>The default value is <code>on</code>.</p>

Variable	Description
<code>enable-implicit-host-preparation=on</code>	<p>Determines whether SnapDrive for UNIX implicitly requests host preparation for LUNs or notifies you that it is required and exits.</p> <ul style="list-style-type: none">• <code>on</code> - SnapDrive for UNIX implicitly requests the host to create more resources, if there is inadequate amount of resources available to create the required number of LUNs. The number of LUNs created is specified in the <code>available-lun-reserve</code> variable. The default value is <code>on</code>.• <code>off</code> - SnapDrive for UNIX informs you if additional host preparation is necessary for LUN creation and SnapDrive exits the operation. You can then perform the operations necessary to free up resources needed for LUN creation. For example, you can execute the <code>snapdrive config prepare luns</code> command. After the preparation is complete, you can reenter the current SnapDrive for UNIX command. <div data-bbox="865 867 1461 1115"><p>This variable applies only to systems where host preparation is needed before you can create LUNs for the hosts that require the preparation. This variable is used only on configurations that include LUNs.</p></div>


Variable	Description
<code>enable-migrate-nfs-version</code>	<p>Allows to clone/restore by using the higher version of NFS.</p> <p>In a pure NFSv4 environment, when snap management operations such as clone and restore are attempted with a Snapshot copy created on NFSv3, snap management operation fails.</p> <p>The default value is <code>off</code>. During this migration, only the protocol version is considered and other options such as <code>rw</code> and <code>largefiles</code> are not taken into account by SnapDrive for UNIX.</p> <p>Therefore, only the NFS version for the corresponding NFS filespec is added in the <code>/etc/fstab</code> file. Ensure that the appropriate NFS version is used to mount the file specification by using <code>-o vers=3</code> for NFSv3 and <code>-o vers=4</code> for NFSv4. If you want to migrate the NFS file specification with all the mount options, it is recommended to use <code>-mntopts</code> in the snap management operations. It is mandatory to use <code>nfs</code> in the attribute value of the Access Protocol in the export policy rules of the parent volume during migration in clustered Data ONTAP .</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Ensure that you use only the <code>nfsvers</code> or <code>vers</code> commands as the mount options, to check the NFS version.</p> </div>
<code>enable-mountguard-support</code>	<p>Enables SnapDrive for UNIX support for the Mount Guard feature of AIX, which prevents simultaneous or concurrent mounts. If a file system is mounted on one node and the variable is enabled, AIX prevents the same file system from being mounted on another node. By default the <code>enable-mountguard-support</code> variable is set to <code>off</code>.</p>
<code>enable-ping-to-check-filer-reachability</code>	<p>If the ICMP protocol access is disabled or ICMP packets are dropped between the host and storage system network where SnapDrive for UNIX is deployed, this variable must be set to <code>off</code>, so that SnapDrive for UNIX does not ping to check if the storage system is reachable or not. If this variable is set to on only SnapDrive snap connect operation does not work due to the ping failure. By default, this variable is set to <code>on</code></p>


Variable	Description
<pre>enable-split-clone=off</pre>	<p>Enables splitting the cloned volumes or LUNs during Snapshot connect and Snapshot disconnect operations, if this variable is set to <code>on</code> or <code>sync</code>. You can set the following values for this variable:</p> <ul style="list-style-type: none"> • <code>on</code> - enables an asynchronous split of cloned volumes or LUNs. • <code>sync</code> - enables a synchronous split of cloned volumes or LUNs. • <code>off</code> - disables the split of cloned volumes or LUNs. The default value is <code>off</code>. <p>If you set this value to <code>on</code> or <code>sync</code> during the Snapshot connect operation and <code>off</code> during the Snapshot disconnect operation, SnapDrive for UNIX does not delete the original volume or LUN that is present in the Snapshot copy.</p> <p>You can also split the cloned volumes or LUNs by using the <code>-split</code> option.</p>
<pre>enforce-strong-ciphers=off</pre>	<p>Set this variable to <code>on</code> for the SnapDrive daemon to enforce TLSv1 to communicate with the client.</p> <p>It enhances the security of communication between the client and the SnapDrive daemon using better encryption.</p> <p>By default, this option is set to <code>off</code>.</p>
<pre>filer-restore-retries=140</pre>	<p>Specifies the number of times SnapDrive for UNIX attempts to restore a Snapshot copy on a storage system if a failure occurs during the restore. The default value is <code>140</code>.</p> <p>In normal circumstances, the default value should be adequate. Under other circumstances, this operation could fail because the storage system is exceptionally busy. If it keeps failing even though the LUNs are online and correctly configured, you might want to increase the number of retries.</p>


Variable	Description
<code>filer-restore-retry-sleep-secs=15</code>	<p>Specifies the number of seconds SnapDrive for UNIX waits between attempts to restore a Snapshot copy. The default value is <code>15</code> seconds.</p> <p>In normal circumstances, the default value should be adequate. Under other circumstances, this operation could fail because the storage system is exceptionally busy. If it keeps failing even though the LUNs are online and correctly configured, you might want to increase the number of seconds between retries.</p>
<code>filesystem-freeze-timeout-secs=300</code>	<p>Specifies the number of seconds that SnapDrive for UNIX waits between attempts to access the file system. The default value is <code>300</code> seconds.</p> <p>This variable is used only on configurations that include LUNs.</p>
<code>flexclone-writereserve-enabled=on</code>	<p>It can take any one of the following values:</p> <ul style="list-style-type: none"> • <code>on</code> • <code>off</code> <p>Determines the space reservation of the FlexClone volume created. Acceptable values are <code>on</code> and <code>off</code>, based on the following rules.</p> <ul style="list-style-type: none"> • Reservation: on • Optimal: file • Unrestricted: volume • Reservation: off • Optimal: file • Unrestricted: none

Variable	Description
<pre>fstype=jfs2</pre>	<p>Specifies the type of file system that you want to use for SnapDrive for UNIX operations. The file system must be a type that SnapDrive for UNIX supports for your operating system.</p> <p>AIX: <code>jfs</code>, <code>jfs3</code> or <code>vxfs</code></p> <p>The default value is <code>jfs2</code>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>The JFS file system type is supported only for Snapshot operations and not for storage operations.</p> </div> <p>You can also specify the type of file system that you want to use by using the <code>-fstype</code> option through CLI.</p>
<pre>lun-onlining-in-progress-sleep-secs=3</pre>	<p>Specifies the number of seconds between retries during attempts to bring back online a LUN after a volume-based SnapRestore operation. The default value is <code>3</code>.</p>
<pre>lun-on-onlining-in-progress-retries=40</pre>	<p>Specifies the number of retries during attempts to bring back online a LUN after a volume-based SnapRestore operation. The default value is <code>40</code>.</p>
<pre>mgmt-retry-sleep-secs=2</pre>	<p>Specifies the number of seconds SnapDrive for UNIX waits before retrying an operation on the Manage ONTAP control channel. The default value is <code>2</code> seconds.</p>
<pre>mgmt-retry-sleep-long-secs=90</pre>	<p>Specifies the number of seconds SnapDrive for UNIX waits before retrying an operation on the Manage ONTAP control channel after a failover error message occurs. The default value is <code>90</code> seconds.</p>

Variable	Description
<code>multipathing-type=NativeMPIO</code>	<p>Specifies the multipathing software to use. The default value depends on the host operating system. This variable applies only if one of the following statements is true:</p> <ul style="list-style-type: none"> • More than one multipathing solution is available. • The configurations include LUNs. <p>The acceptable values are <code>none</code> or <code>nativempio</code>.</p> <p>You can set the following values for this variable:</p> <p>AIX: The value you set for AIX depends on which protocol you are using.</p> <ul style="list-style-type: none"> • If you are using FCP, set this to any one of the following values: <ul style="list-style-type: none"> ◦ NativeMPIO The default value is <code>none</code>. • In addition, set the <code>default-transport</code> option to FCP. • If you are using iSCSI, set this value to <code>none</code>. In addition, set the <code>default-transport</code> option to <code>iscsi</code>.
<code>override-vbsr-snapmirror-check</code>	<p>You can set the value of the <code>override-vbsr-snapmirror-check</code> variable to <code>on</code> to override the SnapMirror relationship, when a Snapshot copy to be restored is older than the SnapMirror baseline Snapshot copy, during volume-based SnapRestore (VBSR). You can use this variable only if the OnCommand Data Fabric Manager (DFM) is not configured.</p> <p>By default, the value is set to <code>off</code>. This variable is not applicable for clustered Data ONTAP version 8.2 or later.</p>
<code>PATH="/sbin:/usr/sbin:/bin:/usr/lib/vxvm/ bin:/usr/bin:/opt/NTAPontap/SANToolkit/ bin:/opt/NTAPsanlun/bin:/opt/VRTS/bin:/etc/vx/bin"</code>	<p>Specifies the search path the system uses to look for tools.</p> <p>You should verify that this is correct for your system. If it is incorrect, change it to the correct path.</p> <p>The default value might vary depending on your operating system. This path is the default for</p> <p>AIX host does not use this variable because they process the commands differently.</p>


Variable	Description
<pre data-bbox="134 163 621 195">/opt/NetApp/snapdrive/.pwfile</pre>	<p data-bbox="816 163 1495 226">Specifies the location of the password file for the user login for the storage systems.</p> <p data-bbox="816 260 1495 323">The default value might vary depending on your operating system.</p> <p data-bbox="816 357 1495 464">The default path for Linux is <code>/opt/NetApp/snapdrive/.pwfile/opt/ontap/snapdrive/.pwfile</code></p>
<pre data-bbox="134 527 654 558">ping-interfaces-with-same-octet</pre>	<p data-bbox="816 516 1495 856">Avoids unnecessary pings through all the available interfaces in the host that might have different subnet IPs configured. If this variable is set to <code>on</code>, SnapDrive for UNIX considers only the same subnet IPs of the storage system and pings the storage system to verify address response. If this variable is set to <code>off</code>, SnapDrive takes all the available IPs in the host system and pings the storage system to verify address resolution through each subnet, which may be locally detected as a ping attack.</p>
<pre data-bbox="134 919 402 951">prefix-filer-lun</pre>	<p data-bbox="816 909 1495 1014">Specifies the prefix that SnapDrive for UNIX applies to all LUN names it generates internally. The default value for this prefix is an empty string.</p> <p data-bbox="816 1047 1495 1176">This variable allows the names of all LUNs created from the current host, but not explicitly named on a SnapDrive for UNIX command line, to share an initial string.</p> <div data-bbox="865 1224 930 1287" style="display: inline-block; vertical-align: middle;">  </div> <p data-bbox="1008 1224 1463 1287" style="margin-left: 20px;">This variable is used only on configurations that include LUNs.</p>
<pre data-bbox="134 1360 418 1392">prefix-clone-name</pre>	<p data-bbox="816 1350 1495 1455">The string given is appended with the original storage system volume name, to create a name for the FlexClone volume.</p>

Variable	Description
<code>prepare-lun-count=16</code>	<p>Specifies how many LUNs SnapDrive for UNIX should prepare to create. SnapDrive for UNIX checks this value when it receives a request to prepare the host to create additional LUNs.</p> <p>The default value is <code>16</code>, which means the system is able to create 16 additional LUNs after the preparation is complete.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>This variable applies only to systems where host preparation is needed before you can create LUNs. This variable is used only on configurations that include LUNs. hosts require that preparation.</p> </div>
<code>rbac-method=dfm</code>	<p>Specifies the access control methods. The possible values are <code>native</code> and <code>dfm</code>.</p> <p>If the variable is set to <code>native</code>, the access-control file that is stored in <code>/vol/vol0/sdprbac/sdhost-name.prbac</code> or <code>/vol/vol0/sdprbac/sdgeneric-name.prbac</code> is used for access checks.</p> <p>If the variable is set to <code>dfm</code>, Operations Manager is a prerequisite. In such a case, SnapDrive for UNIX issues access checks to Operations Manager.</p>
<code>rbac-cache=off</code>	<p>Specifies whether to enable or disable cache. SnapDrive for UNIX maintains a cache of access check queries and the corresponding results. SnapDrive for UNIX uses this cache only when all the configured Operations Manager servers are down.</p> <p>You can set the value of the variable to either <code>on</code> to enable cache, or to <code>off</code> to disable it. The default value is <code>off</code>, which configures SnapDrive for UNIX to use Operations Manager and the set <code>rbac-method</code> configuration variable to <code>dfm</code>.</p>
<code>rbac-cache-timeout</code>	<p>Specifies the rbac cache timeout period and is applicable only when <code>rbac-cache</code> is enabled. The default value is <code>24</code> hrs. SnapDrive for UNIX uses this cache only when all the configured Operations Manager servers are down.</p>

Variable	Description
<pre>recovery-log- file=/var/log/sdrecovery.log</pre>	<p>Specifies where SnapDrive for UNIX writes the recovery log file.</p> <p>The default value depends on your host operating system. The path shown in this example is the default path for a AIX host.</p>
<pre>recovery-log-save=20</pre>	<p>Specifies how many old recovery log files SnapDrive for UNIX should save. After this limit is reached, SnapDrive for UNIX discards the oldest file when it creates a new one.</p> <p>SnapDrive for UNIX rotates this log file each time it starts a new operation. The default value is <code>20</code>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>You should use the default value. If you decide to change the default, remember that having too many large log files can take up space on your disk and might eventually affect performance.</p> </div>
<pre>san-clone-method</pre>	<p>Specifies the type of clone that you can create.</p> <p>It can take the following values:</p> <ul style="list-style-type: none"> • <code>lunclone</code> <p>Allows a connection by creating a clone of the LUN in the same storage system volume. The default value is <code>lunclone</code>.</p> • <code>optimal</code> <p>Allows a connection by creating a restricted FlexClone volume of the storage system volume.</p> • <code>unrestricted</code> <p>Allows a connection by creating an unrestricted FlexClone volume of the storage system volume.</p>

Variable	Description
<pre>secure-communication-among- clusternodes=on</pre>	<p>Specifies a secure communication within the host cluster nodes for remote execution of SnapDrive for UNIX commands.</p> <p>You can direct SnapDrive for UNIX to use RSH or SSH by changing the value of this configuration variable. The RSH or SSH methodology adopted by SnapDrive for UNIX for remote execution is determined only by the value set in the installation directory of the <code>snapdrive.conf</code> file of the following two components:</p> <ul style="list-style-type: none"> • The host on which the SnapDrive for UNIX operation is executed, to get the host WWPN information and device path information of remote nodes. <p>For example, <code>snapdrive storage create</code> executed on master host cluster node uses the RSH or SSH configuration variable only in the local <code>snapdrive.conf</code> file to do either of the following:</p> <ul style="list-style-type: none"> ◦ Determine the remote communication channel. ◦ Execute the <code>devfsadm</code> command on remote nodes. • The non-master host cluster node, if the SnapDrive for UNIX command is to be executed remotely on the master host cluster node. <p>To send the SnapDrive for UNIX command to the master host cluster node, the RSH or SSH configuration variable in the local <code>snapdrive.conf</code> file is consulted to determine the RSH or SSH mechanism for remote command execution.</p> <p>The default value of <code>on</code> means that SSH is used for remote command execution. The value <code>off</code> means that RSH is used for execution.</p>


Variable	Description
<code>snapcreate-cg-timeout=relaxed</code>	<p>Specifies the interval that the <code>snapdrive snap create</code> command allows for a storage system to complete fencing. Values for this variable are as follows:</p> <ul style="list-style-type: none"> • <code>urgent</code> - specifies a short interval. • <code>medium</code> - specifies an interval between urgent and relaxed. • <code>relaxed</code> - specifies the longest interval. This value is the default. <p>If a storage system does not complete fencing within the time allowed, SnapDrive for UNIX creates a Snapshot copy using the methodology for Data ONTAP versions before 7.2.</p>
<code>snapcreate-check-nonpersistent-nfs=on</code>	<p>Enables and disables the Snapshot create operation to work with a non-persistent NFS file system. Values for this variable are as follows:</p> <ul style="list-style-type: none"> • <code>on</code> - SnapDrive for UNIX checks whether NFS entities specified in the <code>snapdrive snap create</code> command are present in the file system mount table. The Snapshot create operation fails if the NFS entities are not persistently mounted through the file system mount table. This is the default value. • <code>off</code> - SnapDrive for UNIX creates a Snapshot copy of NFS entities that do not have a mount entry in the file system mount table. <p>The Snapshot restore operation automatically restores and mounts the NFS file or directory tree that you specify.</p> <p>You can use the <code>-nopersist</code> option in the <code>snapdrive snap connect</code> command to prevent NFS file systems from adding mount entries in the file system mount table.</p>
<code>snapcreate-consistency-retry-sleep=1</code>	<p>Specifies the number of seconds between best-effort Snapshot copy consistency retries. The default value is <code>1</code> second.</p>

Variable	Description
<pre>snapconnect-nfs-removedirectories=off</pre>	<p>Determines whether SnapDrive for UNIX deletes or retains the unwanted NFS directories from the FlexClone volume during the Snapshot connect operation.</p> <ul style="list-style-type: none"> • <code>on</code> - Deletes the unwanted NFS directories (storage system directories not mentioned in the <code>snapdrive snap connect</code> command) from the FlexClone volume during the Snapshot connect operation. <p>The FlexClone volume is destroyed if it is empty during the Snapshot disconnect operation.</p> <ul style="list-style-type: none"> • <code>off</code> - Retains the unwanted NFS storage system directories during the Snapshot connect operation. The default value is <code>off</code>. <p>During the Snapshot disconnect operation, only the specified storage system directories are unmounted from the host. If nothing is mounted from the FlexClone volume on the host, the FlexClone volume is destroyed during the Snapshot disconnect operation.</p> <p>If you set this variable to <code>off</code> during the connect operation or <code>on</code> during the disconnect operation, the FlexClone volume is not to be destroyed, even if it has unwanted storage system directories and is not empty.</p>
<pre>snapcreate-must-make-snapinfo-on-qtrees=off</pre>	<p>Set this variable to <code>on</code> to enable the Snapshot create operation to create Snapshot copy information about a qtree. The default value is <code>off</code> (disabled).</p> <p>SnapDrive for UNIX always attempts to write snapinfo at the root of a qtree if the LUNs are still snapped and are at the qtree. When you set this variable to <code>on</code>, SnapDrive for UNIX fails the Snapshot create operation if it cannot write this data. You should set this variable only to <code>on</code> if you are replicating Snapshot copies using qtree SnapMirror.</p> <div data-bbox="867 1692 932 1759" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1008 1675 1461 1776" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>Snapshot copies of qtrees work the same way Snapshot copies of volumes do.</p> </div>


Variable	Description
<code>snapcreate-consistency-retries=3</code>	<p>Specifies the number of times SnapDrive for UNIX attempts a consistency check on a Snapshot copy after it receives a message that a consistency check failed.</p> <p>This variable is particularly useful on host platforms that do not include a freeze function. This variable is used only on configurations that include LUNs.</p> <p>The default value is <code>3</code>.</p>
<code>snapdelete-delete-rollback-withsnap=off</code>	<p>Set this value to <code>on</code> to delete all rollback Snapshot copies related to a Snapshot copy. Set it to <code>off</code> to disable this feature. The default value is <code>off</code>.</p> <p>This variable takes effect only during a Snapshot delete operation and is used by the recovery log file if you encounter a problem with an operation.</p> <p>It is best to accept the default setting.</p>
<code>snapmirror-dest-multiple-filervolumesenabled=off</code>	<p>Set this variable to <code>on</code> to restore Snapshot copies that span multiple storage systems or volumes on (mirrored) destination storage systems. Set it to <code>off</code> to disable this feature. The default value is <code>off</code>.</p>
<code>snaprestore-delete-rollback-afterrestore=off</code>	<p>Set this variable to <code>on</code> to delete all rollback Snapshot copies after a successful Snapshot restore operation. Set it to <code>off</code> to disable this feature. The default value is <code>off</code> (enabled).</p> <p>This option is used by the recovery log file if you encounter a problem with an operation.</p> <p>It is best to accept the default value.</p>


Variable	Description
<code>snaprestore-make-rollback=on</code>	<p>Set this value to either <code>on</code> to create a rollback Snapshot copy or <code>off</code> to disable this feature. The default value is <code>on</code>.</p> <p>A rollback is a copy of the data that SnapDrive makes on the storage system before it begins a Snapshot restore operation. If a problem occurs during the Snapshot restore operation, you can use the rollback Snapshot copy to restore the data to the state it was in before the operation began.</p> <p>If you do not want the extra security of a rollback Snapshot copy at restore time, set this option to <code>off</code>. If you want the rollback, but not enough for your Snapshot restore operation to fail if you cannot make one, set the variable <code>snaprestore-must-makerollback</code> to <code>off</code>.</p> <p>This variable is used by the recovery log file, which you send to NetApp technical support if you encounter a problem.</p> <p>It is best to accept the default value.</p>
<code>snaprestore-must-make-rollback=on</code>	<p>Set this variable to <code>on</code> to cause a Snapshot restore operation to fail if the rollback creation fails. Set it to <code>off</code> to disable this feature. The default value is <code>on</code>.</p> <ul style="list-style-type: none"> • <code>on</code> - SnapDrive for UNIX attempts to make a rollback copy of the data on the storage system before it begins the Snapshot restore operation. If it cannot make a rollback copy of the data, SnapDrive for UNIX halts the Snapshot restore operation. • <code>off</code> - Use this value if you want the extra security of a rollback Snapshot copy at restore time, but not enough for the Snapshot restore operation to fail if you cannot make one. <p>This variable is used by the recovery log file if you encounter a problem with an operation.</p> <p>It is best to accept the default value.</p>

Variable	Description
<code>snaprestore-snapmirror-check=on</code>	<p>Set this variable to <code>on</code> to enable the <code>snapdrive snap restore</code> command to check the SnapMirror destination volume. If it is set to <code>off</code>, the <code>snapdrive snap restore</code> command is unable to check the destination volume. The default value is <code>on</code>.</p> <p>If the value of this configuration variable is <code>on</code> and the SnapMirror relationship state is <code>broken-off</code>, the restore can still proceed.</p>
<code>space-reservations-enabled=on</code>	<p>Enables space reservation when creating LUNs. By default, this variable is set to <code>on</code>; therefore, the LUNs created by SnapDrive for UNIX have space reservation.</p> <p>You can use this variable to disable the space reservation for LUNs created by the <code>snapdrive snap connect</code> command and <code>snapdrive storage create</code> command. It is best to use the <code>-reserve</code> and <code>-noreserve</code> command-line options to enable or disable LUN space reservation in the <code>snapdrive storage create</code>, <code>snapdrive snap connect</code>, and <code>snapdrive snap restore</code> commands.</p> <p>SnapDrive for UNIX creates LUNs, resizes storage, makes Snapshot copies, and connects or restores the Snapshot copies based on the space reservation permission that is specified in this variable or by the of <code>-reserve</code> or <code>-noreserve</code> command-line options. It does not consider the storage system-side thin provisioning options before performing the preceding tasks.</p>
<code>trace-enabled=on</code>	<p>Set this variable to <code>on</code> to enable the trace log file, or to <code>off</code> to disable it. The default value is <code>on</code>. Enabling this file does not affect performance.</p>

Variable	Description
<pre>trace-level=7</pre>	<p>Specifies the types of messages SnapDrive for UNIX writes to the trace log file. This variable accepts the following values:</p> <ul style="list-style-type: none"> • 1 - Record fatal errors • 2 - Record admin errors • 3 - Record command errors • 4 - Record warnings • 5 - Record information messages • 6 - Record in verbose mode • 7 - Full diagnostic output <p>The default value is 7.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>It is best not to change the default value. Setting the value to something other than 7 does not gather adequate information for a successful diagnosis.</p> </div>
<pre>trace-log-file=/var/log/sd-trace.log</pre>	<p>Specifies where SnapDrive for UNIX writes the trace log file.</p> <p>The default value varies depending on your host operating system.</p> <p>The path shown in this example is the default path for an AIX host.</p>

Variable	Description
<pre>trace-log-max-size=0</pre>	<p>Specifies the maximum size of the log file in bytes. When the log file reaches this size, SnapDrive for UNIX renames it and starts a new log file.</p> <div data-bbox="863 373 932 436" style="float: left; margin-right: 10px;">  </div> <div data-bbox="1003 302 1461 504" style="border: 1px solid #ccc; padding: 5px; margin-left: 20px;"> <p>However, no new trace log file is created when the trace log file reaches the maximum size. For the daemon trace log file, new log file is created when the log file reaches the maximum size.</p> </div> <p>The default value is <code>0</code>. SnapDrive for UNIX never starts a new log file in the middle of an operation. The actual size of the file could vary slightly from the value specified here.</p> <div data-bbox="863 802 932 865" style="float: left; margin-right: 10px;">  </div> <div data-bbox="1003 730 1461 932" style="border: 1px solid #ccc; padding: 5px; margin-left: 20px;"> <p>It is best to use the default value. If you change the default, remember that too many large log files can take up space on your disk and might eventually affect performance.</p> </div>
<pre>trace-log-save=100</pre>	<p>Specifies how many old trace log files SnapDrive for UNIX should save. After this limit is reached, SnapDrive for UNIX discards the oldest file when it creates a new one. This variable works with the <code>tracelog-max-size</code> variable. By default, <code>trace-logmax-size=0</code> saves one command in each file, and <code>trace-log-save=100</code> retains the last 100 log files.</p>
<pre>use-https-to-dfm=on</pre>	<p>Specifies whether you want SnapDrive for UNIX to use SSL encryption (HTTPS) to communicate with Operations Manager.</p> <p>The default value is <code>on</code>.</p>

Variable	Description
<code>use-https-to-filer=on</code>	<p>Specifies whether you want SnapDrive for UNIX to use SSL encryption (HTTPS) when it communicates with the storage system.</p> <p>The default value is <code>on</code>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>If you are using a version of Data ONTAP earlier to 7.0, you might see slower performance with HTTPS enabled. Slow performance is not an issue if you are running Data ONTAP 7.0 or later.</p> </div>
<code>vmtype=lvm</code>	<p>Specify the type of volume manager you want to use for SnapDrive for UNIX operations. The volume manager must be a type that SnapDrive for UNIX supports for your operating system. Following are the values that you can set for this variable, and the default value varies depending on the host operating systems:</p> <ul style="list-style-type: none"> • AIX: <code>vxvm</code> or <code>lvm</code> <p>The default value is <code>lvm</code></p> <p>You can also specify the type of volume manager that you want to use by using the <code>-vmtype</code> option.</p>

Variable	Description
<code>vol-restore</code>	<p>Determines whether SnapDrive for UNIX should perform volume-based snap restore (vbsr) or single-file snap restore (sfsr).</p> <p>The following are the possible values.</p> <ul style="list-style-type: none"> • <code>preview</code> - Specifies that SnapDrive for UNIX initiates a volume-based SnapRestore preview mechanism for the given host file specification. • <code>execute</code> - Specifies that SnapDrive for UNIX proceeds with volume based SnapRestore for the specified filespec. • <code>off</code> - Disables the vbsr option and enables the sfsr option. The default value is <code>off</code>. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>If the variable is set to <code>preview/execute</code>, then you cannot override this setting by using CLI to perform SFSR operations.</p> </div>
<code>volmove-cutover-retry=3</code>	<p>Specifies the number of times SnapDrive for UNIX retries the operation during the volume migration cut-over phase.</p> <p>The default value is <code>3</code>.</p>
<code>volmove-cutover-retry-sleep=3</code>	<p>Specifies the number of seconds SnapDrive for UNIX waits between the volume-move-cutover-retry operation.</p> <p>The default value is <code>3</code>.</p>
<code>volume-clone-retry=3</code>	<p>Specifies the number of times, SnapDrive for UNIX retries the operation during FlexClone creation.</p> <p>The default value is <code>3</code>.</p>
<code>volume-clone-retry-sleep=3</code>	<p>Specifies the number of seconds, SnapDrive for UNIX waits between the retries during FlexClone creation.</p> <p>The default value is <code>3</code>.</p>

What the SnapDrive configuration wizard does

The SnapDrive configuration wizard enables you to configure SnapDrive for UNIX, and the NFS or SAN settings, depending on the environment. Alternatively, you can also open

the `snapdrive.conf` file and edit the configuration variables.

SnapDrive configuration wizard

Use the SnapDrive configuration wizard to update the configuration variables in the wizard. You can run the configuration wizard at any time to modify your configuration changes to SnapDrive.

You can run the configuration wizard from `/opt/NetApp/snapdrive/setup/config_wizard`.

Enter `exit` to close the configuration wizard, without saving the changes.

Alternatively, you can modify the configuration variables value directly in the `snapdrive.conf` file.

Related information

[Stack requirements](#)

Some configuration commands

There are few commands that help you in configuring SnapDrive for UNIX.

The following table summarizes additional commands that are helpful in configuring SnapDrive for UNIX:

Command or action	Description
Configuring and verifying your version of SnapDrive for UNIX software	
<code>snapdrive config show</code>	Check the values in the <code>snapdrive.conf</code> file.
<code>snapdrive version</code>	Check the version of SnapDrive for UNIX.
<code>snapdrived start</code>	Start the SnapDrive for UNIX daemon.
<code>snapdrive config prepare luns -count count_value</code>	Prepare the host for creating a specific number of LUNs as well as to determine how many LUNs you can create.
<code>snapdrive clone split</code>	Estimate, start, stop, and query the status of split for a volume clone or a LUN clone.
Edit the variables in the <code>snapdrive.conf</code> file.	Change the path name and options for the log files. SnapDrive for UNIX logs information to three files: <ul style="list-style-type: none">• An audit file• A recovery file• A trace file

Command or action	Description
Setting and displaying access control permissions between a host and a storage system.	
Edit the access control permissions file (<code>sd <i>hostname</i>.prbac</code>) on the storage system associated with that host.	Specify the access control permissions a host has on a storage system. You can set the following access levels for a host on a storage system: <ul style="list-style-type: none"> • NONE—No access. • SNAP CREATE—Create Snapshot copies. • SNAP USE—Delete and rename Snapshot copies. • SNAP ALL—Create, restore, delete, and rename Snapshot copies. • STORAGE CREATE DELETE—Create, resize, and delete storage. • STORAGE USE—Connect and disconnect storage. • STORAGE ALL—Create, delete, connect, and disconnect storage. • ALL ACCESS—All operations.
<code>snapdrive config access show <filer_name></code>	Display information about the access control permissions a host has to a storage system.
<code>snapdrive config delete <filename> [<filename> . . .]</code>	Remove the specified user name-password pair from SnapDrive for UNIX.

Using the SnapDrive configuration wizard

The configuration wizard allows you to configure in NFS, SAN or Mixed environment.

Steps to configure in NFS environment

The following are the steps to configure in NFS environment.

Steps

1. Select the **NFS** profile.
2. Enable the Protection Manager Integration.
 - Select **Yes** to enable the access permission checks by using the DataFabric Manager.
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the `http/https` port to communicate with the DataFabric Manager. The default value is `8088`.
 - Enter the SSL server port to access the DataFabric Manager. The default value is `8488`.

- Enable the HTTPs enabled to communicate with the DataFabric Manager.
 - Select **No** to enable the access permission checks by using the rbac.
3. Specify the role-based access control methods. The possible values are **native** and **dfm**.
- Select **native** to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`.
 - Select **dfm** to check the access permission using the Operations Manager console.



If you select **dfm** as **rbac-method** without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as **dfm** without enabling Protection Manager Integration is displayed.

4. Specify **https** or **http** to communicate with the storage system.
5. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.
- If you select **Yes**, the SnapDrive daemon is restarted and the configuration changes are reflected.
 - If you select **No**, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

Steps to configure in SAN environment

The following are the steps to configure in SAN environment.

Steps

1. Select the SAN profile.
2. Select the required transport protocol.
 - Select **fc** to set the default-transport.
 - Select **iscsi** to set the default-transport.
3. Select the SAN Storage Stack (combination of MPIO Solution, volume manager, and file system). The options are **native**, **veritas**, and **none**.

SnapDrive does not support veritas for iSCSI transport protocol.

4. Enable the Protection Manager Integration.
 - Select **Yes** to enable the access permission checks by using the DataFabric Manager.
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the **http/https** port to communicate with the DataFabric Manager. The default value is **8088**.
 - Enter the SSL server port to access the DataFabric Manager. The default value is **8488**.
 - Enable the HTTPs enabled to communicate with the DataFabric Manager
 - Select **No** to enable the access permission checks by using the rbac.
5. Specify the role-based access control methods. The possible values are **native** and **dfm**.
 - Select **native** to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`

`/vol/vol0/sdprbac/sdgenericname.prbac`.

- Select `dfm` to check the access permission using the Operations Manager.



If you select `dfm` as `rbac-method` without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as `dfm` without enabling Protection Manager Integration is displayed.

6. Specify `https` or `http` to communicate with the storage system.
7. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.
 - If you select `Yes`, the SnapDrive daemon is restarted and the configuration changes are reflected.
 - If you select `No`, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

Steps to configure in Mixed SAN and NFS environment

The following are the steps to configure in Mixed SAN and NFS environment.

Steps

1. Select the Mixed profile.
2. Select the required transport protocol.
 - Select `fc` to set the default-transport.
 - Select `iscsi` to set the default-transport.
3. Select the SAN Storage Stack (combination of MPIO Solution, volume manager, file system). The options are `native`, `veritas`, and `none`.

SnapDrive does not support veritas for iSCSI transport protocol.

4. Enable the Protection Manager Integration.
 - Select `Yes` to enable the access permission checks by using the DataFabric Manager
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the `http/https` port to communicate with the DataFabric Manager. The default value is `8088`.
 - Enter the SSL server port to access the DataFabric Manager. The default value is `8488`.
 - Enable the HTTPs enabled to communicate with the DataFabric Manager.
 - Select `No` to enable the access permission checks by using the `rbac`.
5. Specify the role-based access control methods. The possible values are `native` and `dfm`.
 - Select `native` to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`
 - Select `dfm` to check the access permission using the Operations Manager console.



If you select `dfm` as `rbac-method` without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as `dfm` without enabling Protection Manager Integration is displayed.

6. Specify `https` or `http` to communicate with the storage system.
7. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.
 - If you select `Yes`, the SnapDrive daemon is restarted and the configuration changes are reflected.
 - If you select `No`, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

SnapDrive modifies the following variables in the `snapdrive.conf` file.

- `contact-http-dfm-port`
- `contact-ssl-dfm-port`
- `use-https-to-dfm`
- `default-transport`
- `use-https-to-filer`
- `fstype`
- `multipathing-type`
- `vmtype`
- `rbac-method`
- `rbac-cache`

Setting values in the `snapdrive.conf` file

You can change the values in the `snapdrive.conf` file or add new name-value pairs.

You must be logged in as a root user.

Steps

1. Back up the `snapdrive.conf` file.
2. Open the `snapdrive.conf` file in a text editor.
3. To add a name-value pair, use the following format:

```
config-option-name=value value # optional comment
```

`config-option-name` is the name of the variable you want to configure; for example, `audit-log-file`.
`value` is the value you want to assign to this option.

If you want to include a comment with the name-value pair, precede the comment with a number sign (`#`).

You should enter only one name-value pair, per line.

If the name or the value uses a string, enclose the string in either single (') or double (") quotation marks. You can place the quotation marks either around the entire name-value pair or around only the value. The following examples show how you can use quotation marks and comments with name-value pairs:

```
"config-option-one=string with white space" # double quotes around the pair
```

```
config-option-two="string with white space" # double quotes around the value
```

```
config-option-2B='string with white space' # single quotes around the value
```

4. To modify a name-value pair, replace the current value with the new value.

Follow the steps below to ensure that the default values are recorded in the file.

- a. Add the sign (#) to the line that you want to modify.
- b. Copy the line.
- c. Activate the copied text by removing the number sign (#).
- d. Modify the value.

If you want to specify a blank value (for example, to disable the audit log file), enter a pair of double quotation marks ("").

5. Save the file after you make your changes.

SnapDrive for UNIX automatically checks this file each time it starts. Your changes take effect the next time it starts.

6. Restart the SnapDrive for UNIX daemon by using the `snapdrived restart` command.

Restarting the daemon is necessary for `snapdrive.conf` file changes to take effect.

Checking the version of SnapDrive for UNIX

You can verify the version of SnapDrive for UNIX by entering the `snapdrive version` command.

Steps

1. At the CLI prompt, enter the following command:

```
snapdrive version
```

Example

```
# snapdrive version
snapdrive Version 5.2
snapdrive Daemon Version 5.2
```



The only argument this command accepts is `-v`, which displays additional version details. If you include additional arguments, SnapDrive for UNIX displays a warning and then the version number.

Configuration information for Vserver

You must configure Vserver in SnapDrive for UNIX, to perform SnapDrive operations.

To configure Vserver with SnapDrive for UNIX, in clustered DATA ONTAP, ensure that the IP address of the Vserver's management logical interface (LIF) is mapped with the Vserver name, either in Domain Name Service (DNS) or in the `/etc/hosts` file. You must also ensure that the Vserver name is configured in SnapDrive for UNIX by using the following command:

```
snapdrive config set <vsadmin> <Vserver name>
```

Related information

[Support for Vserver](#)

Login information for the Vserver

A user name and password allows SnapDrive for UNIX to access the Vserver. It also provides security because, in addition to being logged in as a vsadmin, you must run SnapDrive for UNIX and provide the correct user name and password whenever prompted.

Specifying login information for the Vserver

You must specify the user login information for the Vserver. Depending on what you specified when you set up the Vserver, each Vserver must use the configured Vserver user name. If there is a change in your Vserver name, you must ensure that the new Vserver name is configured in SnapDrive for UNIX.

Steps

1. Enter the following command:

```
snapdrive config set user_name filename [filename...]
```

- *user_name* is the user name that was specified for the Vserver when you first set it up. The default user is vsadmin. *filename* is the Vserver name.
- *filer_name* allows you to enter multiple Vservers on one command line if they all have the same user login or password. You must enter at least one Vserver name.

```
# snapdrive config set vsadmin clstr-vs2
Password for vsadmin:
Retype password:
```

Verifying login information for Vserver

You can verify if the Vserver is configured in SnapDrive for UNIX using the `snapdrive config list` command.

Steps

1. Enter the following command: `snapdrive config list`

This command displays the user name or Vserver specified in SnapDrive for UNIX, and does not display the passwords for the Vserver.

The following example displays the *vsadmin* as a *StorageSystem*.

```
# snapdrive config list
username      appliance name  appliance type
-----
vsadmin       clstr-vs2       StorageSystem
```

Deleting a user from a Vserver

You can delete login information from a Vserver by executing the `snapdrive config delete` command.

Steps

1. Enter the following command:

```
snapdrive config delete appliance_name
```

appliance_name is the name of the Vserver on which you want to delete login information.

```
# snapdrive config delete clstr-vs2
Deleted configuration for appliance: clstr-vs2
```

SnapDrive for UNIX removes the login information for the Vserver you specify.

Audit, recovery, and trace logging in SnapDrive for UNIX

SnapDrive for UNIX helps you maintain various types of log files such as audit, recovery, and trace log files. These log files are used later for troubleshooting.

Types of logs

SnapDrive for UNIX supports various types of log files, which help you troubleshoot when SnapDrive for UNIX is not working as expected.

- Audit log

SnapDrive for UNIX logs all commands and their return codes in an audit log. SnapDrive for UNIX makes an entry when you initiate a command and another when the command is complete. The later entry includes both the status of the command and the completion time.

- Recovery log

Some SnapDrive for UNIX operations have the potential to leave the system in an inconsistent or less

usable state if interrupted. This situation could occur if a user terminates the program, or if the host crashes in the middle of an operation. The recovery log contains the steps of a Snap restore operation. It documents the steps that are taken and the progress made so that technical support can assist you with the manual recovery process.

- Trace log

SnapDrive for UNIX reports information useful for diagnosing problems. If you have a problem, NetApp technical support might request this log file.

SnapDrive 4.0 for UNIX introduced SnapDrive for UNIX daemon service. For SnapDrive for UNIX commands to run, the daemon must be running. Daemon tracing must be carried out on for each individual command, even when commands are run in parallel. The location and name of the log file is `/var/log/sd-trace.log`. These trace files have only the command-specific trace entries. The trace logs for daemon execution are recorded in a different trace file `/var/log/sd-daemon-trace.log`.


Enabling and disabling log files

If you want to enable a log file, specify a file name as the value in the name-value pair of the log file you want to enable. If you want to disable a file, do not enter a value for the log file name parameter.

You must have logged in as a root user.

Steps

1. Open the `snapdrive.conf` file in a text editor.
2. Choose the appropriate option to either enable or disable a log file.

If you want to...	Then...
Enable a log file	<p>Specify a file name as the value in the name-value pair of the log file you want to enable. SnapDrive for UNIX only writes log files if it has the name of a file to write to. The default names for the log files are as follows:</p> <ul style="list-style-type: none">• Audit log: <code>sd-audit.log</code>• Recovery log: <code>sd-recovery.log</code>• Trace log: <code>sd-trace.log</code> <div data-bbox="889 1591 954 1654"></div> <p data-bbox="1032 1579 1458 1675">The path to these files might vary depending on your host operating system.</p>

If you want to...	Then...
<p>Disable a log file</p>	<p>Do not enter a value for the log file name parameter. If you do not supply a value, there is no file name to which SnapDrive for UNIX can write the log information.</p> <p>Example This example disables the audit log file.</p> <pre>audit-log-file=""</pre>

3. Save the `snapdrive.conf` file after you make all your changes.

SnapDrive for UNIX automatically checks this file each time it starts. You must restart the SnapDrive for UNIX daemon for the changes to take effect.

Log file rotation settings

The values you specify for the variable in the `snapdrive.conf` file affect the log file rotation.

The values you specify in the `snapdrive.conf` file enable automatic log file rotations. You can change these values, if necessary, by editing the `snapdrive.conf` variables. The following options affect log file rotation:

- `audit-log-max-size`
- `audit-log-save`
- `trace-max-size`
- `trace-log-max-save`
- `recovery-log-save`

With automatic log rotation, SnapDrive for UNIX keeps old log files until it reaches the limit specified in the `audit-log-save`, `trace-log-save`, and `recovery-log-save` variable. Then it deletes the oldest log file.

SnapDrive for UNIX tracks which file is oldest by assigning the file the number "0" when it creates the file. Each time it creates a new file, it increments by 1 the number assigned to each of the existing log files. When a log file's number reaches the save value, SnapDrive for UNIX deletes that file.

Example: This example uses the `ls` command to display information about the log files on the system.

Based on those settings, you would see the following information in log files.


```
# ls -l /var/log/sd*
-rw-r--r-- 1 root other 12247 Mar 13 13:09 /var/log/sd-audit.log
-rw-r--r-- 1 root other 20489 Mar 12 16:57 /var/log/sd-audit.log.0
-rw-r--r-- 1 root other 20536 Mar 12 03:13 /var/log/sd-audit.log.1
-rw-r--r-- 1 root other 3250 Mar 12 18:38 /var/log/sd-recovery.log.1
-rw-r--r-- 1 root other 6250 Mar 12 18:36 /var/log/sd-recovery.log.2
-rw-r--r-- 1 root other 6238 Mar 12 18:33 /var/log/sd-recovery.log.3
-rw-r--r-- 1 root other 191704 Mar 13 13:09 /var/log/sd-trace.log
-rw-r--r-- 1 root other 227929 Mar 12 16:57 /var/log/sd-trace.log.0
-rw-r--r-- 1 root other 213970 Mar 12 15:14 /var/log/sd-trace.log.1
-rw-r--r-- 1 root other 261697 Mar 12 14:16 /var/log/sd-trace.log.2
-rw-r--r-- 1 root other 232904 Mar 12 14:15 /var/log/sd-trace.log.3
-rw-r--r-- 1 root other 206905 Mar 12 14:14 /var/log/sd-trace.log.4
```

Contents of an audit log file

The audit log shows information about commands you issued with SnapDrive for UNIX.

The audit log file maintains the history of the following information:

- The commands issued.
- The return value from those commands.
- The user ID of the user who invoked the command.
- A timestamp indicating when the command started (with no return code) and another timestamp indicating when the command finished (with a return code). The audit log record shows only information about `snapdrive` use (issued commands).

An audit log file contains the following information.

Field	Description
uid	user ID
gid	group ID
msgText	message text
returnCode	return code from a command

Changing the defaults for the audit logs

You can use `snapdrive.conf` file to change the logging parameters of the audit log files such as maximum size of audit log file, and maximum number of old audit files.

The `snapdrive.conf` file enables you to set the following values for audit logging:

- The maximum size of the audit log file. The default size is 20K. After the file size reaches the value specified in the `snapdrive.conf` file, SnapDrive for UNIX renames the current audit log file by adding an arbitrary number to the name. Then, a new audit file is started using the name specified by the `audit-log-file` value.
- The maximum number of old audit files that SnapDrive for UNIX saves. The default is 2.

Example of an audit log file:

```
2501: Begin uid=0 gid=1 15:35:02 03/12/04 snapdrv snap create -dg
rdg -snapname snap_rdg1
2501: Status=0 15:35:07 03/12/04
2562: Begin uid=0 gid=1 15:35:16 03/12/04 snapdrv snap create -dg
rdg -snapname snap_rdg1
2562: FAILED Status=4 15:35:19 03/12/04
```

The first pair of lines in this example shows an operation that succeeded, as indicated by the "Status=0" line.

The second pair of lines indicates an operation that failed. The return code of "4" means "already exists." If you look at the two command lines, you can see that the first created a Snapshot copy called `snap_rdg1`. The second line attempted to do the same, but the name already existed, so the operation failed.

Contents of the recovery log

The recovery log helps you to trace the reasons for an inconsistent system state. SnapDrive for UNIX generates this file when some operation stops working.

If you press Ctrl-C to halt SnapDrive for UNIX, or if the host or storage system fails in the middle of an operation, the system might not be able to recover automatically.

During any operation that, if interrupted, could leave the system in an inconsistent state, SnapDrive for UNIX writes information to a recovery log file. If a problem occurs, you can send this file to NetApp technical support so they can assist you in recovering the system's state.

The recovery log utility maintains the records of the commands that are issued during the operation. Each command is marked with an `operation_index` (a number that uniquely identifies the operation being executed), followed by the date/time stamp and the message text.

Default values for the recovery logs

You can change the name of the recovery log file and the maximum number of old recovery log files that SnapDrive for UNIX saves.

The `snapdrive.conf` file enables you to set the following values for recovery logging:

- The name of the file containing the recovery log, such as `recovery.log`.
- The maximum number of old recovery files that SnapDrive for UNIX saves. The default is 20. SnapDrive for UNIX keeps this number of recovery logs, if the problem with the process is not identified immediately. SnapDrive for UNIX starts a new recovery log file each time it completes an operation. Then, renames the previous one by adding an arbitrary number to the name, such as `recovery.log.0`, `recovery.log.1`,

and so on.



The size of the recovery log file depends on the operation that is performed. Each recovery log contains information about a single operation. When that operation is complete, SnapDrive for UNIX starts a new recovery log, regardless of how large the previous file was. As a result, there is no maximum size for a recovery log file.

The following sample recovery log shows that SnapDrive for UNIX has restored two Snapshot copies before the operations halted. You could send this recovery log file to technical support for assistance in restoring the remaining Snapshot copies.

```
6719: BEGIN 15:52:21 03/09/04 snapdrive snap restore -dg jssdg -
snapname natasha:/vol/vol1:abort_snap_restore
6719: BEGIN 15:52:27 03/09/04 create rollback snapshot:
natasha:/vol/vol1:abort_snap_restore.RESTORE_ROLLBACK_03092004_155
225
6719: END 15:52:29 03/09/04 create rollback snapshot:
natasha:/vol/vol1:abort_snap_restore.RESTORE_ROLLBACK_03092004_155
225 successful
6719: BEGIN 15:52:29 03/09/04 deactivate disk group: jssdg
6719: BEGIN 15:52:29 03/09/04 stop host volume:
/dev/vx/dsk/jssdg/jvol_1
6719: END 15:52:30 03/09/04 stop host volume:
/dev/vx/dsk/jssdg/jvol_1 successful
6719: BEGIN 15:52:30 03/09/04 unmount file system: /mnt/demo_fs
6719: END 15:52:30 03/09/04 unmount file system: /mnt/demo_fs
successful
6719: BEGIN 15:52:30 03/09/04 stop host volume:
/dev/vx/dsk/jssdg/jvol_2
6719: END 15:52:30 03/09/04 stop host volume:
/dev/vx/dsk/jssdg/jvol_2 successful
6719: BEGIN 15:52:30 03/09/04 deport disk group: jssdg
6719: END 15:52:30 03/09/04 deport disk group: jssdg successful
6719: END 15:52:30 03/09/04 deactivate disk group: jssdg
successful
6719: BEGIN 15:52:31 03/09/04 SFSR of LUN: /vol/vol1/lun1 from
snapshot: abort_snap_restore
6719: END 15:52:31 03/09/04 SFSR of LUN: /vol/vol1/lun1 from
snapshot: abort_snap_restore successful
6719: BEGIN 15:52:47 03/09/04 SFSR of LUN: /vol/vol1/lun2 from
snapshot: abort_snap_restore
6719: END 15:52:47 03/09/04 SFSR of LUN: /vol/vol1/lun2 from
snapshot: abort_snap_restore successful
```

What the trace log file is

Technical support uses the trace log file to troubleshoot problems.

Enabling the trace log file does not affect system performance. By default, this file is enabled. You can disable by setting the `snapdrive.conf trace-enabled` variable to `off`.

Default values for the trace log files

The trace log files allow you to set various parameters and also change them. These parameters must be set in the `snapdrive.conf` file.

The following values must be set in the `snapdrive.conf` file:

- The name of the file containing the trace log.
- The maximum size of the trace log file. The default size is "0 " bytes. This value ensures that each trace log file contains only one SnapDrive for UNIX command.

If you reset the default size to a value other than 0, when the file reaches the size you specified, SnapDrive for UNIX renames the current trace log file by adding an arbitrary number to the name. Then it starts a new trace log file using the name specified by the `trace-log-file` value.

- The maximum number of old trace files that SnapDrive for UNIX saves. The default is 100.
- The types of messages that SnapDrive for UNIX writes to the trace log file. By default, the trace log file contains fatal errors, admin errors, command errors, warnings, and information messages.

What AutoSupport is

AutoSupport allows SnapDrive for UNIX to send any operational failures that is incurred due to SnapDrive is sent to the EMS log view of the storage system in the `/etc/log/ems` file.

How SnapDrive for UNIX uses AutoSupport

AutoSupport messages are logged in the EMS log view of the storage system when the `autosupport-enabled` option is set to on in the `snapdrive.conf` file. By default, this option is set to `on` in the `snapdrive.conf` file. SnapDrive for UNIX sends AutoSupport messages to the storage system, where the messages are logged in the Event Management System (EMS).

An AutoSupport message is sent during any of the following scenarios:

- When an operation is stopped because of an operational failure, an AutoSupport message is sent to the storage system for which the operation failed.
- If multiple storage systems are connected to the host and the operational failure occurs in more than one storage system, SnapDrive for UNIX sends the AutoSupport message to a specific storage system for which the operation fails.
- When a new storage controller is added by using `snapdrive config set <username> <filename>`, SnapDrive for UNIX sends an AutoSupport message to the specified storage system.

- When the SnapDrive daemon is restarted or started, the AutoSupport message is sent to the configured storage system.
- When the `snapdrive storage show -all` command is executed, the AutoSupport message is sent to all the configured storage systems.
- When there is a successful snap create operation, the AutoSupport message is sent to the storage system.

Contents of AutoSupport messages

AutoSupport messages contain the following information.

- Event source
- Event ID
- Version of SnapDrive for UNIX
- Message status: Log level messages, for example 1 for alert, 2 for critical, 3 for error, 4 for warning, 5 for notice, 6 for information, and 7 for debug
- Host name
- Host operating system
- Release version of the host operating system
- Name of the storage system
- Usage of Protection Manager/Role Based Access Control
- Error category
- AutoSupport Flag message entry as FALSE
- Host multipathing type: The value configured in `snapdrive.conf` file is logged. If the assistant is not loaded due to incorrect configuration value, no host multipathing type is logged.
- Host virtualization enabled: This is captured only for VMware guest operating system.
- Protocol: The value configured for `default-transport` in the `snapdrive.conf` file.
- Protection enabled: If OnCommand Data Fabric Manager (DFM) is configured with SnapDrive for UNIX, the value `Yes` is logged.



SnapDrive for UNIX does not verify whether OnCommand DFM is in use.

The following additional information is available when you run the `snapdrive storage show -all` command:

- Type of protocols (FCP/iSCSI): Protocols used to create the luns, if any.
- Number of connected LUNs
- Number of disk or volume groups
- Number of file specifications
- Number of host volumes



When AutoSupport is enabled in SnapDrive for UNIX, upon any operation failures, the error messages are logged in the Event Management System (EVM) storage system. If the error message contains any special characters such as (<, >, &, ', ", \r), garbled values are displayed in the EMS log view of the storage system.

Examples of AutoSupport messages

SnapDrive for UNIX provides examples for different scenarios. The content of an AutoSupport message in all the examples are essentially the same regardless of your operating system.

Example: Adding a new storage system

The following example is a message sent from a host named *aix207-116*:

```
computerName="aix207-116"
  eventSource="snapdrive"
  appVersion="5.2 for UNIX"
  eventID="3"
  category="ohio configured"
  subject="host_name=aix207-116, host_os=AIX, host_os_release=1,
host_os_version=6, No of controller=1, PM/RBAC=native, Host
Virtualization=No, Multipath-type=nativempio, Protection Enabled=No,
Protocol=fcp"
```

Example: Restarting the Daemon

SnapDrive for UNIX sends the following AutoSupport message to the storage system when you restart the daemon:

```
computerName="aix207-116"
  eventSource="snapdrive"
  appVersion="5.2 for UNIX"
  eventID="2"
  category="daemon restarted"
  subject="host_name=aix207-116, host_os=AIX, host_os_release=1,
host_os_version=6, No of controller=1, PM/RBAC=native, Host
Virtualization=No, Multipath-type=nativempio, Protection Enabled=No,
Protocol=fcp"
```

SnapDrive for UNIX sends the following AutoSupport message to the storage system when a storage connect operation fails:

```

computerName="aix207-116"
    eventSource="snapdrive"
    appVersion="5.2 for UNIX"
    eventID="4"
    category="storage connect failed"
    subject="host_name=aix207-116, host_os=AIX, host_os_release=1,
host_os_version=6, No of controller=1, PM/RBAC=native, Host
Virtualization=No, Multipath-type=nativempio, Protection Enabled=No,
Protocol=fcp,1384: LUN /vol/vol0/test1 on storage system ohio already
mapped to initiators in igroup aix207-116_fcp_SdIg at ID 0."/>

```

SnapDrive for UNIX sends the following AutoSupport message to the storage system when a `snap create` operation succeeds:

```

computerName="aix207-116"
    eventSource="snapdrive"
    appVersion="5.2 for UNIX"
    eventID="5"
    category="snap create successful"
    subject="host_name=aix207-116, host_os=AIX, host_os_release=1,
host_os_version=6, No of controller=1, PM/RBAC=native, Host
Virtualization=No, Multipath-type=nativempio, Protection Enabled=No,
Protocol=fcp, snapshot_name=snap1"/>

```

Support for multipath access in SnapDrive for UNIX

SnapDrive for UNIX supports FC multipath access to the storage systems using the standard multipathing software solution. By using multipathing, you can configure multiple network paths between the host and storage system.

Platform	Multipathing solution
AIX	For FC <ul style="list-style-type: none"> • NativeMPIO • DMP

If one path fails, the FC traffic continues on the remaining paths. Multipathing is required if the host has multiple paths to a LUN, and it works by making the underlying paths transparent to the user. If the multipathing solution specified in the configuration file for SnapDrive for UNIX operations is configured and supported, SnapDrive for UNIX uses the specified multipathing solution.

Enabling multipathing

To use multipathing in SnapDrive for UNIX, you must complete steps that include installing and starting the HBA. If you are using a non-NetApp multipathing solution, you must download the software and application package from the HBA vendor's web site.

Your system must be running current versions of FC and iSCSI system components.

[NetApp Interoperability Matrix Tool](#)

Steps

1. Install the supported HBAs before you install the appropriate Host Utilities software.



SnapDrive for UNIX supports multivendor HBAs.

2. Start the HBA service.

If the HBA service is not running, the following error message is displayed when you run SnapDrive for UNIX commands, such as `snapdrive storage create` and `snapdrive config prepare luns`:

```
0001-876 Admin error: HBA assistant not found
```

You must verify that the required number of paths are up and running. You can verify the paths by using the `sanlun` utility, which is included with the Host Utilities software. For example, in the FC multipathing configuration, you can use the `sanlun fcp show adapter -v` command.

In the following example, there are two HBA ports (`fcd0` and `fcd1`) connected to the host that are operational (port state). You can have only one HBA or iSCSI initiator and you must configure multipathing by providing more than one path to the target LUNs.


```
# sanlun fcp show adapter -v
adapter name: fcd0
WWPN: 50060b000038c428
WWNN: 50060b000038c429
driver name: fcd
model: A6826A
model description: Fibre Channel Mass Storage Adapter
(PCI/PCI-X)
serial number: Not Available
hardware version: 3
driver version: @(#) libfcd.a HP Fibre Channel
ISP 23xx & 24xx Driver B.11.23.04
/ux/core/isu/FCD/kern/src/common/wsio/fcd_init.c:Oct 18
2005,08:19:50
firmware version: 3.3.18
Number of ports: 1 of 2
port type: Fabric
port state: Operational
supported speed: 2 GBit/sec
negotiated speed: 2 GBit/sec
OS device name: /dev/fcd0
adapter name: fcd1
WWPN: 50060b000038c42a
WWNN: 50060b000038c42b
driver name: fcd
model: A6826A
model description: Fibre Channel Mass Storage Adapter
(PCI/PCI-X)
serial number: Not Available
hardware version: 3
driver version: @(#) libfcd.a HP Fibre Channel
ISP 23xx & 24xx Driver B.11.23.04
/ux/core/isu/FCD/kern/src/common/wsio/fcd_init.c:Oct 18
2005,08:19:50
firmware version: 3.3.18
Number of ports: 2 of 2 port type: Fabric
port state: Operational
supported speed: 2 GBit/sec
negotiated speed: 2 GBit/sec
OS device name: /dev/fcd1
```

If multipathing is enabled on a host, multiple paths are visible for the same LUN. You can use the `sanlun lun show all` command to verify the paths. In the following example, you can find multiple paths to the same LUN (`fish: /vol/vol1/lun`):

```

filer:          lun-pathname          device filename  adapter  protocol
lun size          lun state
filer_1:        fish/vol/vol1/l1          hdisk36          fcs0
FCP            5m (5242880)          GOOD
filer_2:        fish/vol/vol0/lunKr      hdisk39          fcs0
FCP           100m (104857600)        GOOD
filer_3:        fish/vol/vol0/testaix    hdisk2           fcs0
FCP           200m (209715200)        GOOD
filer_4:        fish/vol/vol1/l1          hdisk45          fcs1
FCP            5m (5242880)          GOOD

```

3. In an FC configuration, zone the host HBA ports and target ports by using the switch zoning configuration.
4. Install and set up the appropriate FC or iSCSI switch.
5. Check the SnapDrive for UNIX stack requirements.
6. Install or upgrade SnapDrive for UNIX.
7. Verify the SnapDrive for UNIX installation.
8. Locate the `snapdrive.conf` file path.
9. Configure the following configuration variables in the `snapdrive.conf` file:

- `multipathing-type`
- `default-transport`
- `fstype`
- `vmtype`

For every host, the multipathing type, transport type, file system, and volume manager type are dependent on each other. The following table describes all the possible combinations:

Host platform	Default transport type	Multipathing type	fstype	vmtype
AIX	FCP	absolute	jfs2 or jfs	lvm
		nativempio	jfs2 or jfs	lvm
		dmp	vxfs	vxvm

The preceding table gives the supported values of the `multipathing-type`, `default-transport`, `fstype`, and `vmtype` configuration variables.

10. Save the `snapdrive.conf` file.

SnapDrive for UNIX automatically checks this file each time it starts. You must restart the SnapDrive for UNIX daemon for the changes to take effect.

Related information

[NetApp Support](#)

[NetApp Interoperability](#)

[AIX Host Utilities 6.0 Installation and Setup Guide](#)

Reason to refresh the DMP paths

On hosts with FC and DMP configurations, the `snapdrive storage delete - lun` command can hang.

The command may hang because of inappropriate installation or configuration of the following components:

- NTAPasl
- Veritas stack (storage foundation)
- Multipathing licenses

You must refresh the DMP paths information properly after any FC path is enabled, disabled, or added. To refresh the DMP paths, execute the following commands in the sequential manner as listed below.

Platform	Command
AIX	<ul style="list-style-type: none">• <code>cfgmg</code>• <code>vxdisk scandisk</code>

Thin provisioning in SnapDrive for UNIX

The thin provisioning feature in SnapDrive for UNIX allows the user to have more storage space for the hosts than is actually available on the storage system.

Within SnapDrive for UNIX, you cannot set the fractional reserve value, and there is no integration with Data ONTAP features such as autodelete and autosize. These Data ONTAP features can be safely used with SnapDrive for UNIX; however, there is no awareness within SnapDrive for UNIX, if an autodelete or autosize event occurs.

Related information

[NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment](#)

Enabling thin provisioning for LUNs

You can use SnapDrive for UNIX to carry out thin provisioning on your storage system. Thin provisioning is also referred as space-reservation.

Steps

1. Set the `space-reservations-enabled` configuration variable value to on.

You can also enable thin provisioning by using the `-reserve` and `-noreserve` parameters.

Parameter override the value mentioned in the `-space-reservations-enabled` variable.

You could use `-reserve` and `-noreserve` with the following commands to enable or disable LUN reservation:

- `snapdrive storage create`
- `snapdrive storage resize`
- `snapdrive snap connect`
- `snapdrive snap restore`

By default, SnapDrive for UNIX enables space reservation for a fresh or new storage create operations. For snap restore and snap connect operations, it uses the space reservation present in the Snapshot copy if the `-reserve` or `-noreserve` parameters are not specified at the command line, or if the value in the configuration file is uncommented.

Enabling thin provisioning for NFS entities

You can use SnapDrive for UNIX to carry out thin provisioning for NFS entities on your storage system. Thin provisioning is referred as space-reservation.

Steps

1. To enable space reservation for snap connect operations, you can enable space reservation for volumes by using the `-reserve` parameter with the commands involving NFS entities. For NFS entities, SnapDrive for UNIX uses the space reservation available in the Snapshot copy if the `-reserve` or `-noreserve` parameters are not specified in a command.

Multiple subnet configuration

Multiple subnets are useful in an environment where you want to separate management traffic and data traffic. This separation creates a more secure environment for managing network traffic. SnapDrive 4.1.1 for UNIX and later versions running on servers in such environments supports all the SnapDrive operations available in stand-alone environments and host and HA pair environments.

Data related to the management of storage systems is transmitted through the management interface. DataFabric Manager, Protection Manager, and SnapDrive for UNIX can be part of the management interface. The data interface is used for data traffic between storage systems.

To configure multiple subnets in your environment, you should use the `mgmtpath` option with the `snapdrive config set` command.

SnapDrive for UNIX does not support operations in a SAN environment where the host name of the storage system is different from the public name, but both names resolve to the same IP address. To work around this situation, you can do one of the following:

- Assign a different IP address for the system name.
- Configure the system so that it does not reply when you try to connect to it.

Configuring management and data interfaces for a storage system

You can configure multiple data interfaces for a single management interface in an NFS environment, so that you can separate management traffic from data traffic on your storage system.

Steps

1. Set the configuration for the new management interface:

```
snapdrive config set root
```

```
# snapdrive config set root f3050-197-91
Password for root:
Retype password:
```

2. Configure the data interface for the new management interface:

```
snapdrive config set
```

```
# snapdrive config set -mgmtpath f3050-197-91 f3050-220-91#
```

In the preceding command, `f3050-197-91` is the management interface and `f3050-220-91` is the data interface.

Viewing all the data interfaces for a management interface

You can view all the data interfaces for a management interface by using the `snapdrive config list` command in an NFS environment.

1. At the CLI, enter the following command:

```
snapdrive config list -mgmtpath
```

```
#snapdrive config list -mgmtpath
system name          management interface  datapath interface
-----
f3050-197-91         10.72.197.91          10.72.220.91|10.72.168.91
```

Deleting a data interface entry for a management interface

You can delete a data interface entry that is associated with a specific management interface in an NFS environment by using the `snapdrive config delete -mgmtpath` command.

1. At the CLI, enter the following command:

```
snapdrive config delete -mgmtpath data_interface
```

```
#snapdrive config delete -mgmtpath f3050-197-91
Deleted configuration for appliance: f3050-197-91
```

LUN names in SAN environment

In all the SAN operations, the format of LUN names should always be of the host name, irrespective of whether it resolves to an IP address. In a pure SAN environment, there is no concept of data path. The management interface mapping must be the same as the data path interface.

config list output in a SAN multiple subnet environment

```
#snapdrive config set -mgmtpath f3050-197-91 f3050-197-91

#snapdrive config list -mgmtpath
system name      management interface  datapath interface
-----
bart             10.72.197.91          10.72.197.91
```

Pure NFS environment

If you configure a system for multiple subnets and one or more NFS volumes are mounted through the management interface, then you should always configure the first data interface as the management interface.

In the following example, the management interface is `10.72.221.19`, and the data interface is `10.72.220.45`.

```
# snapdrive config list
username      appliance name  appliance type
-----
root         10.72.221.19   StorageSystem

# snapdrive config list -mgmtpath
system name      management interface  datapath interface
-----
f2040-221-19    10.72.221.19          10.72.220.45
```

Mixed SAN and NFS environments

In mixed SAN and NFS environments, the management and data interface must be mapped so that the first data interface is the same as the management interface.

In the following example, the management interface is `10.72.197.91`, and the data interface is `a10.72.220.91`.

```
#snapdrive config set -mgmtpath f3050-197-91 f3050-197-91 f3050-197-91
f3050-220-91

#snapdrive config list -mgmtpath
system name          management interface  datapath interface
-----
bart                 10.72.197.91         10.72.197.91|10.72.220.91
```

Automatic detection of host entities

SnapDrive for UNIX automatically detects the configuration of the host entity for some commands. A few `snap storage` commands need only the name of the host entity. In these cases, you do not have to specify the type of the host entity.

The following commands are enabled for automatic detection:

- `storage delete`
- `storage resize`
- `snap create`
- `snap restore`
- `snap connect`
- `snap list`

When the host entity exists, SnapDrive for UNIX automatically detects the type of the host entity. In this case, you need to provide only the name of the host entity; you do not have to specify the type. The SnapDrive `snap` commands and some `storage` commands also need only the name of the host entity; you do not have to specify the type.

Automatic detection of commands takes extra time for SnapDrive 4.1 and later because it collects the details of all the storage resources. If you want a faster response, specify the file specification with the SnapDrive for UNIX commands.

You can enable automatic detection for the storage delete operation by running the `snapdrive storage delete` command.

Example 1:

```
snapdrive storage delete host_dg my_fs -full
```

In the example, `host_dg` and `my_fs` are automatically detected.

Example 2:

```
snapdrive storage delete mydg -fs myfs -full
```

In the example, the `mydg` disk group is automatically detected.

You can enable automatic detection for the storage resize operation by running the `snapdrive storage resize` command.

For example:

```
[root@lnx197-132 ~]# snapdrive storage resize mydg23 -addlun -growby 10m
Auto detecting the type of filespec 'mydg23' in progress ... detected as
disk group
    discovering filer LUNs in disk group mydg23...done
    LUN bart:/vol/voldm/mydg23-1_SdLun ... created

    mapping new lun(s) ... done
    discovering new lun(s) ... done.
    initializing LUN(s) and adding to disk group mydg23...done
Disk group mydg23 has been resized
```

You can enable the automatic detection for the snap create operation by running the `snapdrive snap create` command.

For example:


```
root@lnx197-132 ~]# snapdrive snap create mydg22 mydg23 /mnt/mnt12
-snapname new_snap
Auto detecting the type of filespec 'mydg22' in progress ... detected as
disk group
Auto detecting the type of filespec 'mydg23' in progress ... detected as
disk group
Auto detecting the type of filespec '/mnt/mnt12 ' in progress ... detected
as file system

Starting snap create /dev/mapper/mydg22, /dev/mapper/mydg23, /mnt/mnt12
WARNING: DO NOT CONTROL-C!
        If snap create is interrupted, incomplete snapdrive
        generated data may remain on the filer volume(s)
        which may interfere with other snap operations.
Successfully created snapshot new_snap on bart:/vol/voldm

        snapshot new_snap contains:
        disk group mydg22
        disk group mydg23
        disk group dg121 containing host volumes
                lv121 (filesystem: /mnt/mnt12)
```

You can enable automatic detection for the snap connect operation by running the `snapdrive snap connect` command.

For example:

```

[root@lnx197-132 ~]# snapdrive snap connect mydg22 xxx mydg23 yyy
-snapname bart:/vol/voldm:snap_1
Auto detecting the type of filespec 'mydg22' in progress ... detected as
disk group
Auto detecting the type of filespec 'xxx' in progress ...
    xxx does not exist - Taking xxx as a destination to fspec
mydg22Auto detecting the type of filespec 'mydg23' in progress ...
detected as disk group
Auto detecting the type of filespec 'yyy' in progress ...
    yyy does not exist - Taking yyy as a destination to fspec mydg23
connecting mydg22:
    LUN copy mydg22_SdLun_0 ... created
        (original: bart:/vol/voldm/mydg22_SdLun)

    mapping new lun(s) ... done

connecting mydg23:
    LUN copy mydg23_SdLun_1 ... created
        (original: bart:/vol/voldm/mydg23_SdLun)

    mapping new lun(s) ... done
    discovering new lun(s) ... done
    Importing xxx, yyy
Successfully connected to snapshot bart:/vol/voldm:snap_1
    disk group xxx
    disk group yyy

```

You can enable the automatic detection for the snap restore operation by running the `snapdrive snap restore` command.

For example:

```
snapdrive snap restore bart:/vol/voldm/lun44 /mnt/fs3 fs5_SdDg/fs5_SdHv
fs4_SdDg -snapname bart:/vol/voldm:toi_snap
```

```
Auto detection of file_spec(s) in progress ...
```

- 'bart:/vol/voldm/lun44' detected as LUN.
- '/mnt/fs3' detected as file system.
- 'fs5_SdDg/fs5_SdHv' detected as logical volume.
- 'fs4_SdDg' detected as disk group.

```
Starting to restore /dev/mapper/fs4_SdDg, /mnt/fs3,
/dev/mapper/fs5_SdDg-fs5_SdHv, bart:/vol/voldm/lun44
```

```
WARNING: This can take several minutes.
```

```
DO NOT CONTROL-C!
```

```
If snap restore is interrupted, the filespecs
being restored may have inconsistent or corrupted
data.
```

```
For detailed progress information, see the log file /var/log/sd-
recovery.log
```

```
Importing fs4_SdDg, fs3_SdDg, fs5_SdDg
```

```
Successfully restored snapshot toi_snap on bart:/vol/voldm
```

```
disk group fs4_SdDg containing host volumes
```

```
fs4_SdHv (filesystem: /mnt/fs4)
```

```
disk group fs3_SdDg containing host volumes
```

```
fs3_SdHv (filesystem: /mnt/fs3)
```

```
disk group fs5_SdDg containing host volumes
```

```
fs5_SdHv (filesystem: /mnt/fs5)
```

```
raw LUN: bart:/vol/voldm/lun44
```

SnapDrive does not support automatic detection for snap connect and snap restore operations for incorrect file specification.

You can enable automatic detection for the snap list operation by running the `snapdrive snap list` command.

For example:

```

root@lnx197-132 ~]# snapdrive snap list -snapname bart:/vol/voldm:snap_1

snap name                                host                                date
snapped
-----
-----
bart:/vol/voldm:snap_1                   lnx197-132.xyz.com Apr   9 06:04 mydg22
mydg23 dg121
[root@lnx197-132 ~]# snapdrive snap list mydg23
Auto detecting the type of filespec 'mydg23' in progress ... detected as
disk group

snap name                                host                                date
snapped
-----
-----
bart:/vol/voldm:snap_1                   lnx197-132.xyz.com Apr   9 06:04 mydg22
mydg23 dg121
bart:/vol/voldm:all                       lnx197-132.xyz.com Apr   9 00:16
mydg22 mydg23 fs1_SdDg
bart:/vol/voldm:you                       lnx197-132.xyz.com Apr   8 21:03
mydg22 mydg23
bart:/vol/voldm:snap_2                   lnx197-132.xyz.com Apr   8 18:05
mydg22 mydg23

```

What SnapDrive wizards are

SnapDrive has different wizards that help you to perform a particular SnapDrive operation in an interactive manner.

Operations performed using wizards

You can use different wizards to create storage entities and manipulate SnapDrive for UNIX in an efficient manner.

The following SnapDrive for UNIX commands have an equivalent wizard to perform operations:

- `Astorage create`
- `storage delete`
- `snap restore`
- `snap connect`
- `snap disconnect`

Managing storage using a wizard

You can use the SnapDrive for UNIX wizard to create storage in an interactive and efficient manner. The wizard leads you through a set of questions to help you to create storage.

You can launch the wizard by using the `snapdrive storage wizard create` command.

The following storage management operations can be performed:

- Creating a LUN
- Creating a disk group and automatically setting up the LUN
- Creating a disk group and specifying the LUN.
- Creating a host volume and automatically setting up the LUN
- Creating a host volume and specifying the LUN
- Creating a file system on a LUN and automatically setting up the LUN
- Creating a file system on a LUN and specifying the LUN.
- Creating a file system on a LUN and setting up the LUN automatically with Logical Volume Manager (LVM) and disk group specified
- Creating a file system on a LUN and specifying the LUN with LVM and disk group specified
- Creating a file system on a LUN and setting up the LUN automatically with LVM and host volume specified
- Creating a file system on a LUN and specifying the LUN with LVM and host volume specified

Managing Snapshot copies using a wizard

You can use a wizard to manage Snapshot copies. This wizard runs you through a set of questions and helps you to perform the `snap connect`, `snap restore`, and `snap disconnect` operations.

You can run the wizard by using the `snapdrive snap wizard` command.

The following table lists the different operations and corresponding commands to run the wizard. After launching the wizard, follow the steps in the application window.

Operation	Command
Snapshot restore	<code>snapdrive snap wizard restore</code>
Snapshot connect	<code>snapdrive snap wizard connect</code>
Snapshot connect operation for file system with storage system volume	
Snapshot connect for disk group	

Operation	Command
Snapshot disconnect for LUN	<code>snapdrive snap wizard disconnect</code>
Snapshot disconnect for a disk group	
Snapshot disconnect for host volume	
Snapshot disconnect for file system	

Limitations: In SnapDrive for UNIX 4.1 and later, the `snapdrive snap wizard` command has the following limitations:

- Volume-based SnapRestore is not supported with the `snap wizard restore` command.
- FlexClone® volume is not supported with the `snap wizard connect` command.
- Operations on unresponsive file specifications are not supported with `snap wizard` commands.

Deleting storage using a wizard

You can use the storage delete wizard to perform certain delete operations.

You can start the wizard by using the `snapdrive storage wizard delete` command.

You can delete the following entities:

- A LUN
- A disk group
- A logical volume
- A file system

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.